ADFS 3.0を使用したCisco Unified Communications ManagerでのSAML SSOの設定

内容

概要

このドキュメントでは、Cisco Unified Communication Manager(CUCM)、Cisco Unity Connection(CUC)、Expressway製品でWindows 2012 R2を使用して、Active Directoryフェデレーションサービス(ADFS 3.0)でシングルサインオンを設定する手順について説明します。このドキュメントには、Kerberosを設定する手順も含まれています。

前提条件

要件

シングルサインオン(SSO)およびWindows製品に関する知識があることが推奨されます。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- CUCM 11.5
- CUC 11.5
- Expressway 12
- 次の役割を持つWindows 2012 R2 Server:
  - Active Directory証明書サービス
  - Active Directoryフェデレーションサービス

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定前チェック

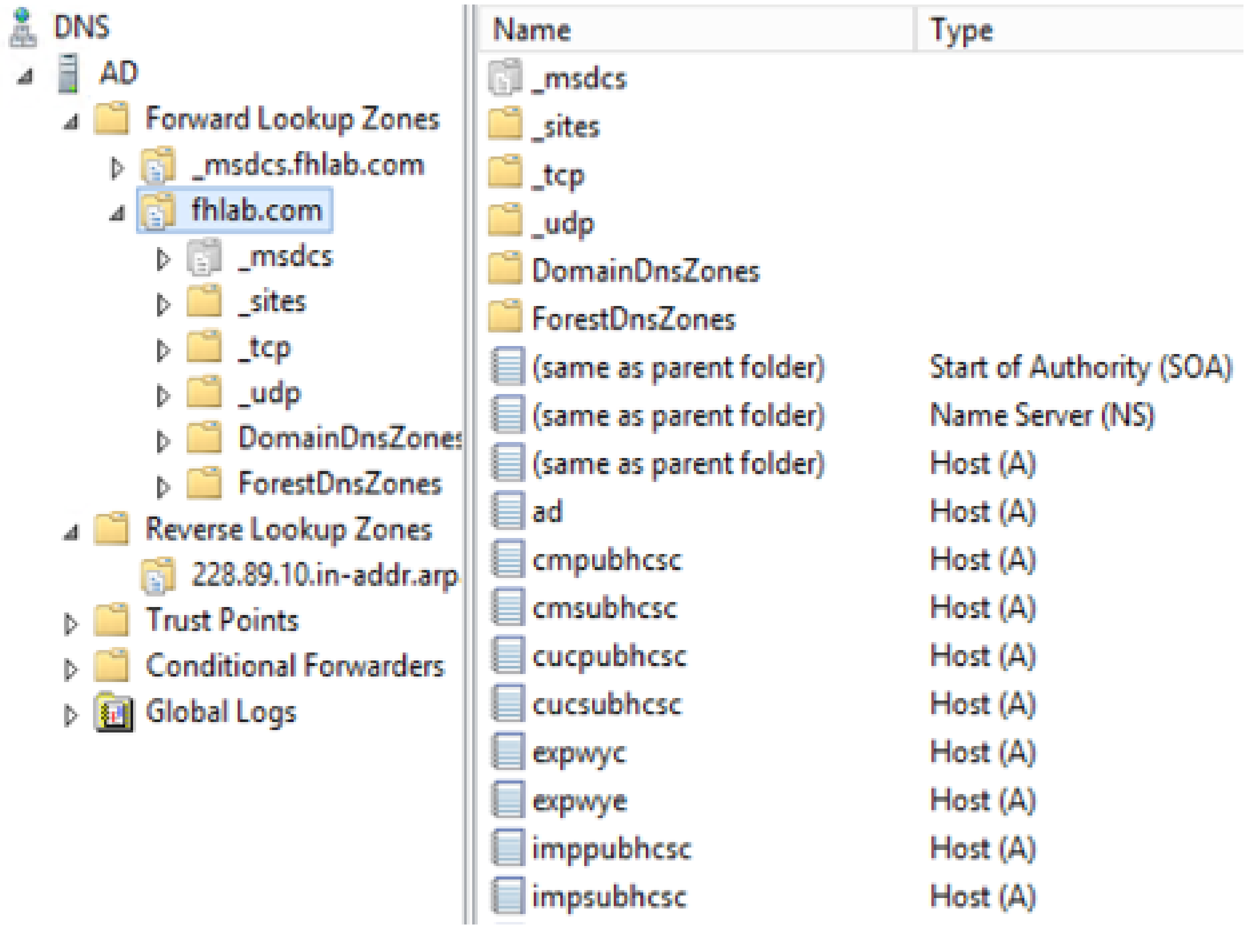
ADFS3をインストールする前に、次のサーバーの役割が環境にすでに存在している必要があります。

· ドメインコントローラとDNS

· すべてのサーバを、ポインタレコード（IPアドレスをドメインまたはホスト名に解決するDNSレコードのタイプ）とともにAレコードとして追加する必要があります

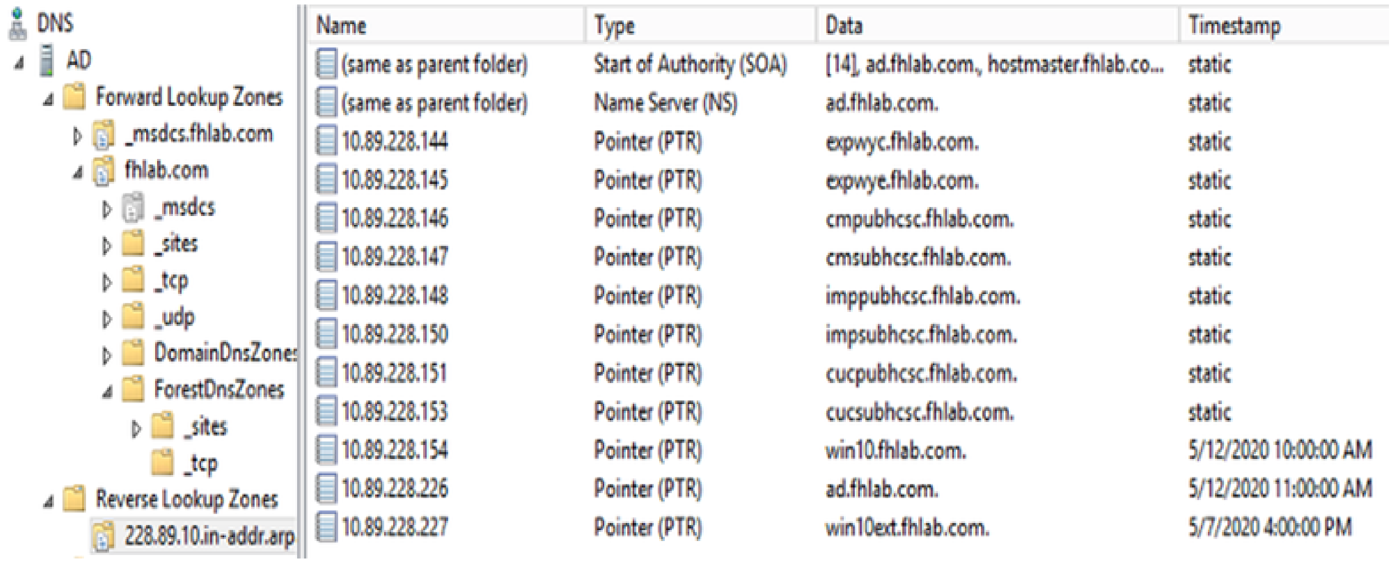
レコード

fhlab.comホストcmpubhcsc、cmsubhcsc、cucpuhcsc、cucsubhcsc、cucsubhcsc、expwyc、 expwye、impuhcsc、imsubhcscが追加されました。



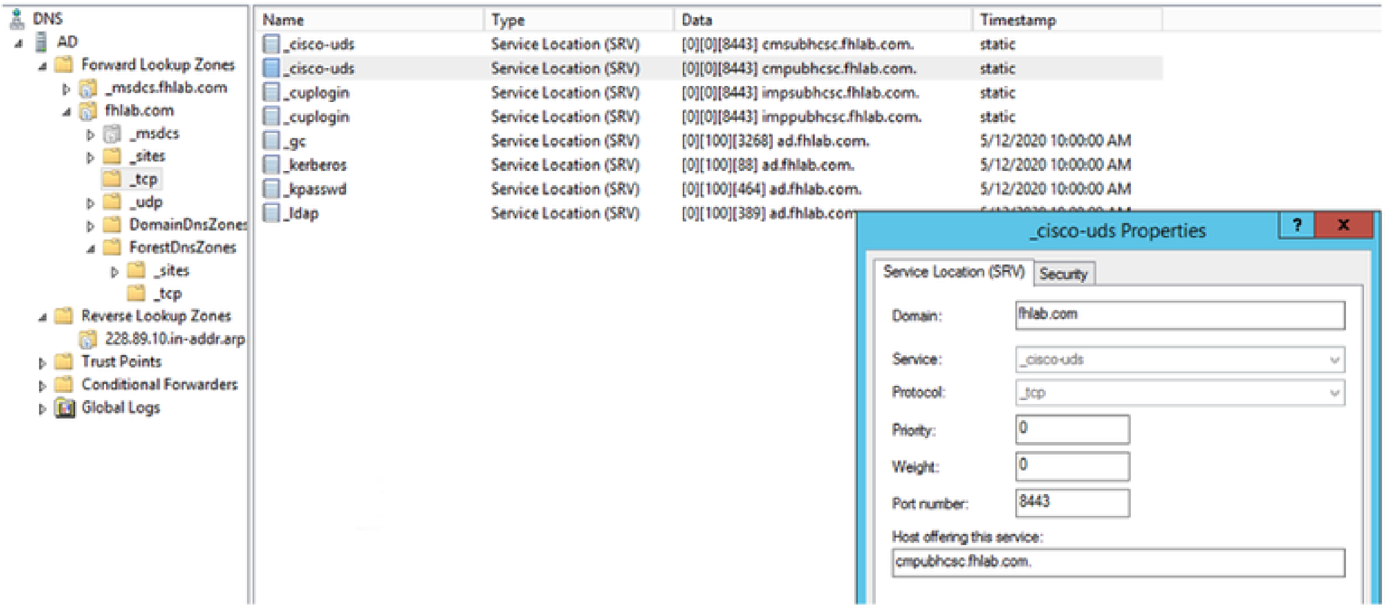
Name	Type
_msdcs	
_sites	
_tcp	
_udp	
DomainDnsZones	
ForestDnsZones	
(same as parent folder)	Start of Authority (SOA)
(same as parent folder)	Name Server (NS)
(same as parent folder)	Host (A)
ad	Host (A)
cmpubhcsc	Host (A)
cmsubhcsc	Host (A)
cucpubhcsc	Host (A)
cucsubhcsc	Host (A)
expwyc	Host (A)
expwye	Host (A)
imppubhcsc	Host (A)
impsubhcsc	Host (A)

ポインタ(PTR)レコード



Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[14], ad.fhlab.com., hostmaster.fhlab.co...	static
(same as parent folder)	Name Server (NS)	ad.fhlab.com.	static
10.89.228.144	Pointer (PTR)	expwyc.fhlab.com.	static
10.89.228.145	Pointer (PTR)	expwye.fhlab.com.	static
10.89.228.146	Pointer (PTR)	cmpubhcsc.fhlab.com.	static
10.89.228.147	Pointer (PTR)	cmsubhcsc.fhlab.com.	static
10.89.228.148	Pointer (PTR)	imppubhcsc.fhlab.com.	static
10.89.228.150	Pointer (PTR)	impsubhcsc.fhlab.com.	static
10.89.228.151	Pointer (PTR)	cucpubhcsc.fhlab.com.	static
10.89.228.153	Pointer (PTR)	cucsubhcsc.fhlab.com.	static
10.89.228.154	Pointer (PTR)	win10.fhlab.com.	5/12/2020 10:00:00 AM
10.89.228.226	Pointer (PTR)	ad.fhlab.com.	5/12/2020 11:00:00 AM
10.89.228.227	Pointer (PTR)	win10ext.fhlab.com.	5/7/2020 4:00:00 PM

Jabber DiscoveryサービスにSRVレコードを配置する必要がある



Name	Type	Data	Timestamp
_cisco-uds	Service Location (SRV)	[0][0][8443] cmsubhcsc.fhlab.com.	static
_cisco-uds	Service Location (SRV)	[0][0][8443] cmpubhcsc.fhlab.com.	static
_cuplogin	Service Location (SRV)	[0][0][8443] impsubhcsc.fhlab.com.	static
_cuplogin	Service Location (SRV)	[0][0][8443] imppubhcsc.fhlab.com.	static
_gc	Service Location (SRV)	[0][100][3268] ad.fhlab.com.	5/12/2020 10:00:00 AM
_kerberos	Service Location (SRV)	[0][100][88] ad.fhlab.com.	5/12/2020 10:00:00 AM
_kpasswd	Service Location (SRV)	[0][100][464] ad.fhlab.com.	5/12/2020 10:00:00 AM
_ldap	Service Location (SRV)	[0][100][389] ad.fhlab.com	

_cisco-uds Properties

Domain: fhlab.com

Service: _cisco-uds

Protocol: _tcp

Priority: 0

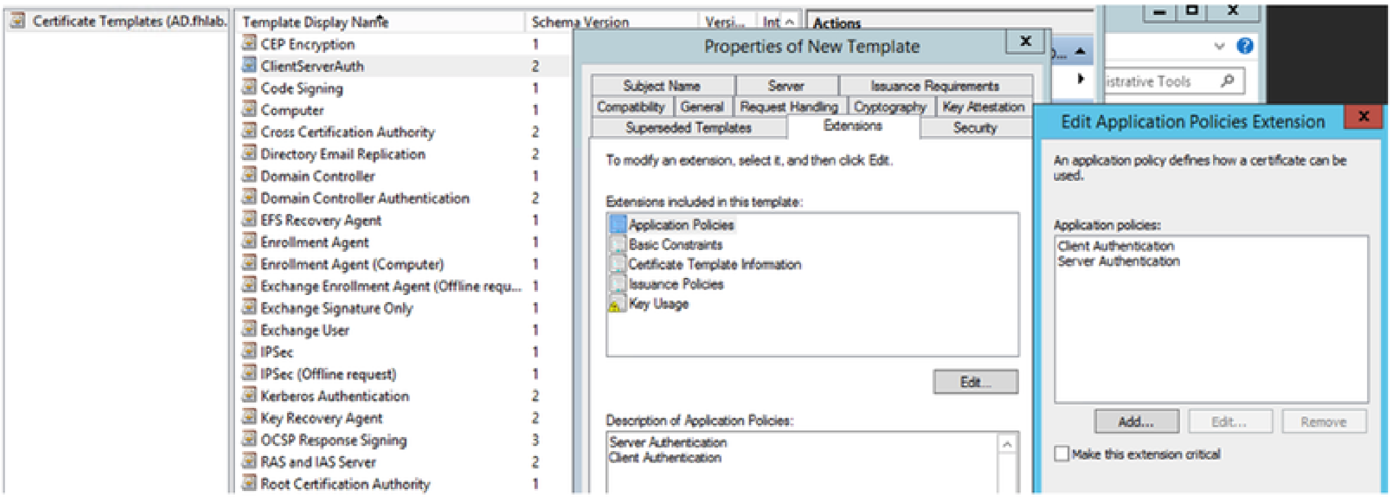
Weight: 0

Port number: 8443

Host offering this service:
cmpubhcsc.fhlab.com.

- ルートCA（証明書がエンタープライズCA署名付きであると仮定）

証明書テンプレートは、Webサーバ証明書テンプレートに基づいて作成する必要があります。証明書テンプレートは、複製、名前変更され、[Extensions]タブで[Application Policies is modified adding a Client Authentication Application Policy]に変更されます。このテンプレートは、内部CAがExpressway E証明書署名要求(CSR)にも署名できるLAB環境のすべての内部証明書（CUCM、CUC、IMP、およびExpressway Core）に署名するために必要です。



Template Display Name	Schema Version	Versi...	Int
CEP Encryption	1		
ClientServerAuth	2		
Code Signing	1		
Computer	1		
Cross Certification Authority	2		
Directory Email Replication	2		
Domain Controller	1		
Domain Controller Authentication	2		
EFS Recovery Agent	1		
Enrollment Agent	1		
Enrollment Agent (Computer)	1		
Exchange Enrollment Agent (Offline requ...	1		
Exchange Signature Only	1		
Exchange User	1		
IPSec	1		
IPSec (Offline request)	1		
Kerberos Authentication	2		
Key Recovery Agent	2		
OCSP Response Signing	3		
RAS and IAS Server	2		
Root Certification Authority	1		

Properties of New Template

To modify an extension, select it, and then click Edit.

Extensions included in this template:
Application Policies
Basic Constraints
Certificate Template Information
Issuance Policies
Key Usage

Description of Application Policies:
Server Authentication
Client Authentication

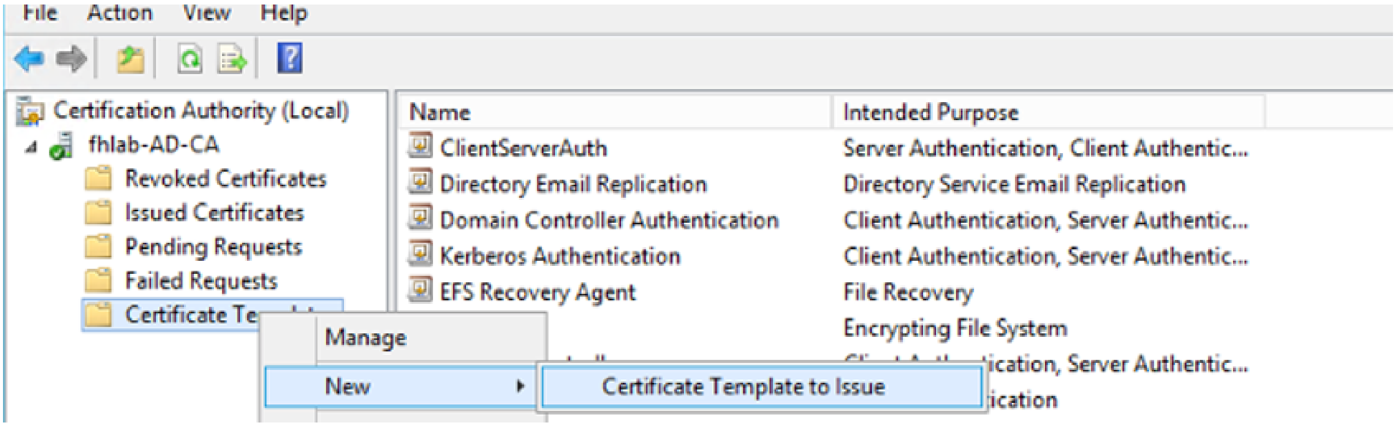
Edit Application Policies Extension

An application policy defines how a certificate can be used.

Application policies:
Client Authentication
Server Authentication

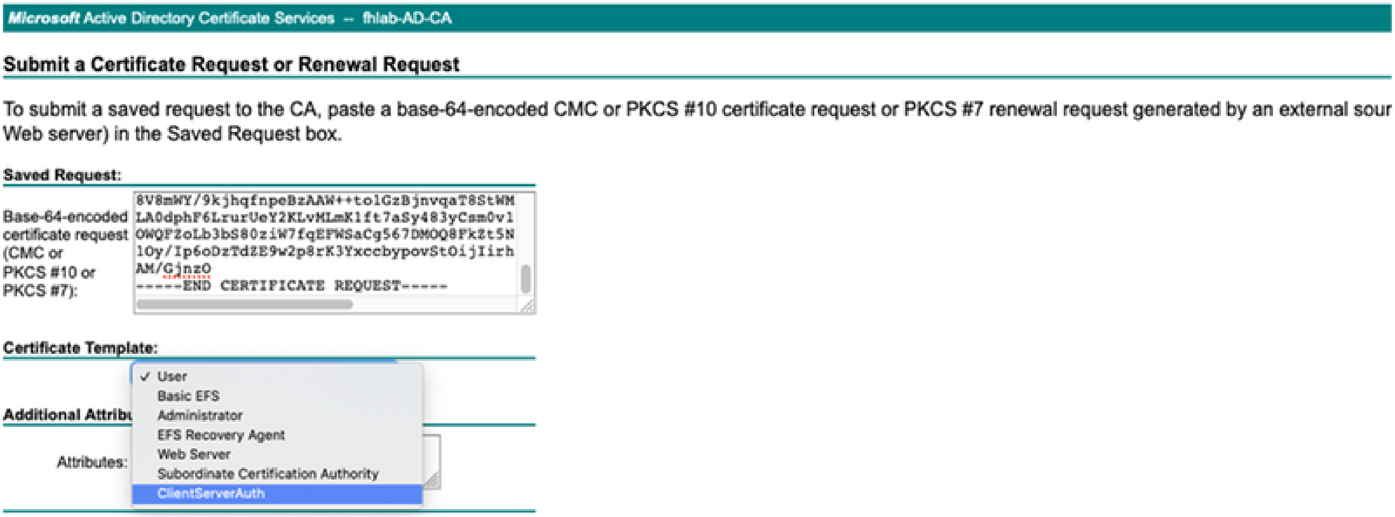
□ Make this extension critical

CSRに署名できるようにするには、作成したテンプレートを発行する必要があります。



Name	Intended Purpose
ClientServerAuth	Server Authentication, Client Authentic...
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authentic...
Kerberos Authentication	Client Authentication, Server Authentic...
EFS Recovery Agent	File Recovery
	Encrypting File System
	ication, Server Authentic...
	ication

CA証明書Webで、以前に作成したテンプレートを選択します。



Microsoft Active Directory Certificate Services -- fhlab-AD-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external sour
Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

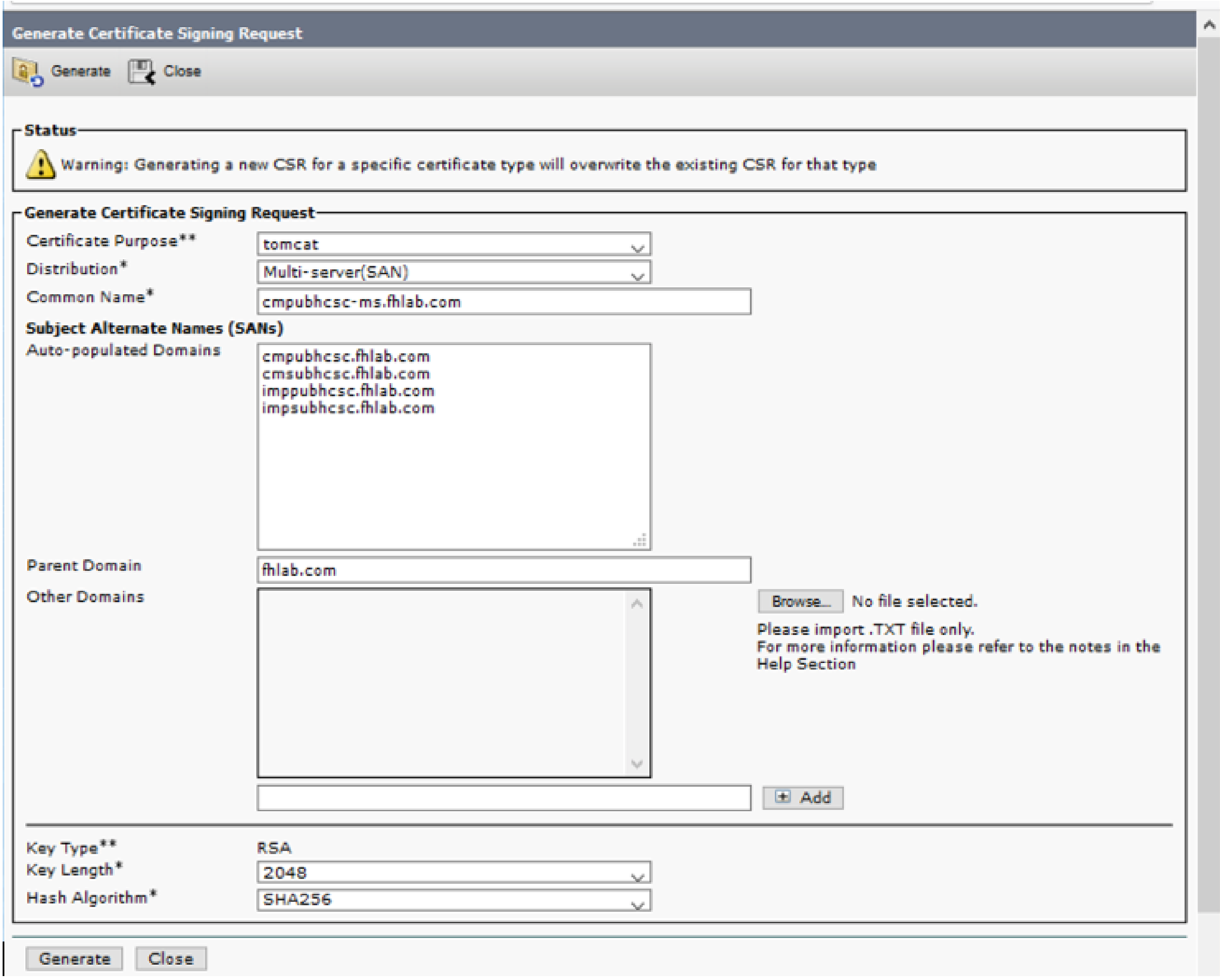
```
8V8mWY/9kjhqfnpeBzAAW++tolGzBjnvqaT8StWM
LA0dphF6LrurUeY2KLvMLmK1ft7aSy483yCsm0v1
OWQFZoLb3bS80ziW7fqEFWSaCg567DMOQ8FkZt5N
1Oy/Ip6oDzTdZE9w2p8rK3YxccbypovStOijIirh
AM/GjnzO
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Additional Attribu

Attributes:

CUCM、IMP、およびCUCマルチサーバCSRは、CAによって生成および署名される必要があります。証明書の目的はtomcatである必要があります。



Generate Certificate Signing Request

Status

Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type

Generate Certificate Signing Request

Certificate Purpose**	tomcat
Distribution*	Multi-server(SAN)
Common Name*	cmpubhcsc-ms.fhlab.com

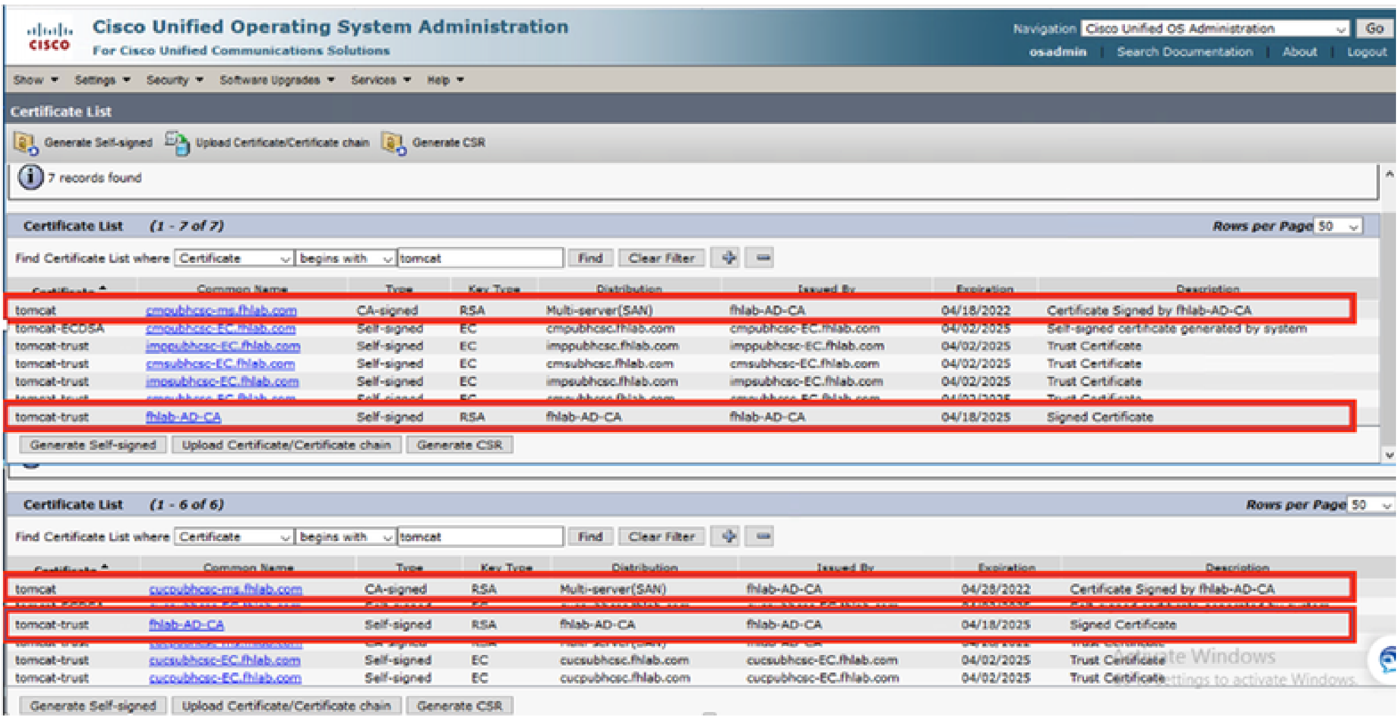
Subject Alternate Names (SANs)

Auto-populated Domains	cmpubhcsc.fhlab.com cmsubhcsc.fhlab.com imppubhcsc.fhlab.com impsubhcsc.fhlab.com
Parent Domain	fhlab.com
Other Domains	

Please import .TXT file only.
For more information please refer to the notes in the Help Section

Key Type**	RSA
Key Length*	2048
Hash Algorithm*	SHA256

CAルート証明書をTomcat信頼にアップロードし、署名付き証明書をtomcatにアップロードする必要があります。


Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified OS Administration Go
osadmin | Search Documentation | About | Logout
Show Settings Security Software Upgrades Services Help
Certificate List
Generate Self-signed
Upload Certificate/Certificate chain
Generate CSR

7 records found

Certificate List (1 - 7 of 7) Rows per Page 50

Find Certificate List where Certificate begins with tomcat Find Clear Filter

Certificate	Common Name	Type	Key Type	Distribution	Issued By	Expiration	Description
tomcat	cmpubhcsc-ms.fhlab.com	CA-signed	RSA	Multi-server(SAN)	fhlab-AD-CA	04/18/2022	Certificate Signed by fhlab-AD-CA
tomcat-ECDSA	cmpubhcsc-EC.fhlab.com	Self-signed	EC	cmpubhcsc.fhlab.com	cmpubhcsc-EC.fhlab.com	04/02/2025	Self-signed certificate generated by system
tomcat-trust	imppubhcsc-EC.fhlab.com	Self-signed	EC	imppubhcsc.fhlab.com	imppubhcsc-EC.fhlab.com	04/02/2025	Trust Certificate
tomcat-trust	cmsubhcsc-EC.fhlab.com	Self-signed	EC	cmsubhcsc.fhlab.com	cmsubhcsc-EC.fhlab.com	04/02/2025	Trust Certificate
tomcat-trust	impsubhcsc-EC.fhlab.com	Self-signed	EC	impsubhcsc.fhlab.com	impsubhcsc-EC.fhlab.com	04/02/2025	Trust Certificate
tomcat-trust	fhlab-AD-CA	Self-signed	RSA	fhlab-AD-CA	fhlab-AD-CA	04/18/2025	Signed Certificate

Generate Self-signed Upload Certificate/Certificate chain Generate CSR

Certificate List (1 - 6 of 6) Rows per Page 50

Find Certificate List where Certificate begins with tomcat Find Clear Filter

Certificate	Common Name	Type	Key Type	Distribution	Issued By	Expiration	Description
tomcat	cucpubhcsc-ms.fhlab.com	CA-signed	RSA	Multi-server(SAN)	fhlab-AD-CA	04/28/2022	Certificate Signed by fhlab-AD-CA
tomcat-trust	fhlab-AD-CA	Self-signed	RSA	fhlab-AD-CA	fhlab-AD-CA	04/18/2025	Signed Certificate
tomcat-trust	cucsubhcsc-EC.fhlab.com	Self-signed	EC	cucsubhcsc.fhlab.com	cucsubhcsc-EC.fhlab.com	04/02/2025	Trust Certificate
tomcat-trust	cucpubhcsc-EC.fhlab.com	Self-signed	EC	cucpubhcsc.fhlab.com	cucpubhcsc-EC.fhlab.com	04/02/2025	Trust Certificate

Generate Self-signed Upload Certificate/Certificate chain Generate CSR

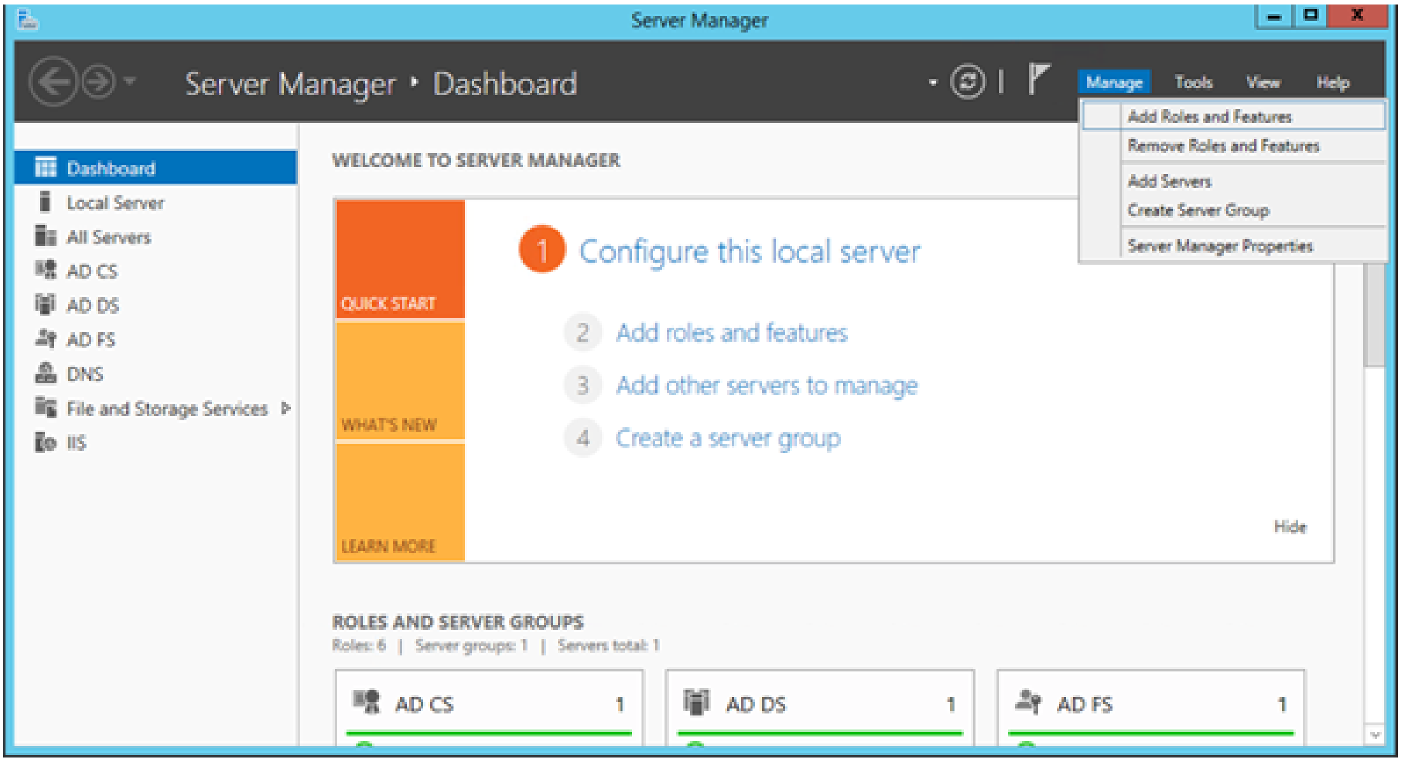
- IIS

そうでない場合は、このセクションでこれらのロールのインストールについて説明します。それ以外の場合は、このセクションをスキップして、MicrosoftからのADFS3のダウンロードに直接進んでください。

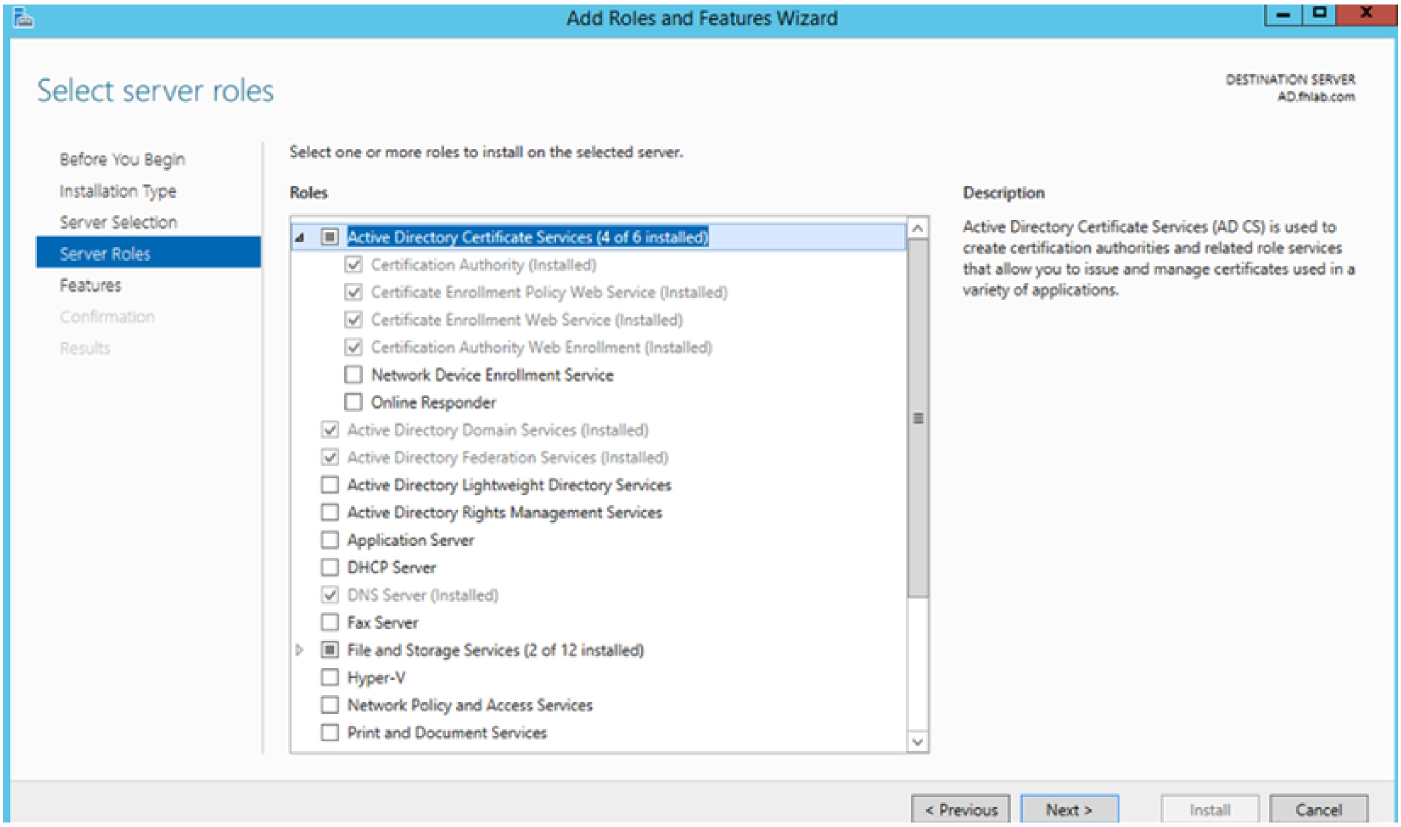
DNSを使用してWindows 2012 R2をインストールした後、サーバをドメインコントローラに昇格します。

次に、Microsoft証明書サービスをインストールします。

[Server Manager]に移動し、新しいロールを追加します。



Active Directory証明書サービスの役割を選択します。



Select server roles

DESTINATION SERVER
AD.fhlab.com

Select one or more roles to install on the selected server.

Roles

- ▣ Active Directory Certificate Services (4 of 6 installed)
  - ☑ Certification Authority (Installed)
  - ☑ Certificate Enrollment Policy Web Service (Installed)
  - ☑ Certificate Enrollment Web Service (Installed)
  - ☑ Certification Authority Web Enrollment (Installed)
  - ☐ Network Device Enrollment Service
  - ☐ Online Responder
- ☑ Active Directory Domain Services (Installed)
- ☑ Active Directory Federation Services (Installed)
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☐ DHCP Server
- ☑ DNS Server (Installed)
- ☐ Fax Server
- ▣ File and Storage Services (2 of 12 installed)
- ☐ Hyper-V
- ☐ Network Policy and Access Services
- ☐ Print and Document Services

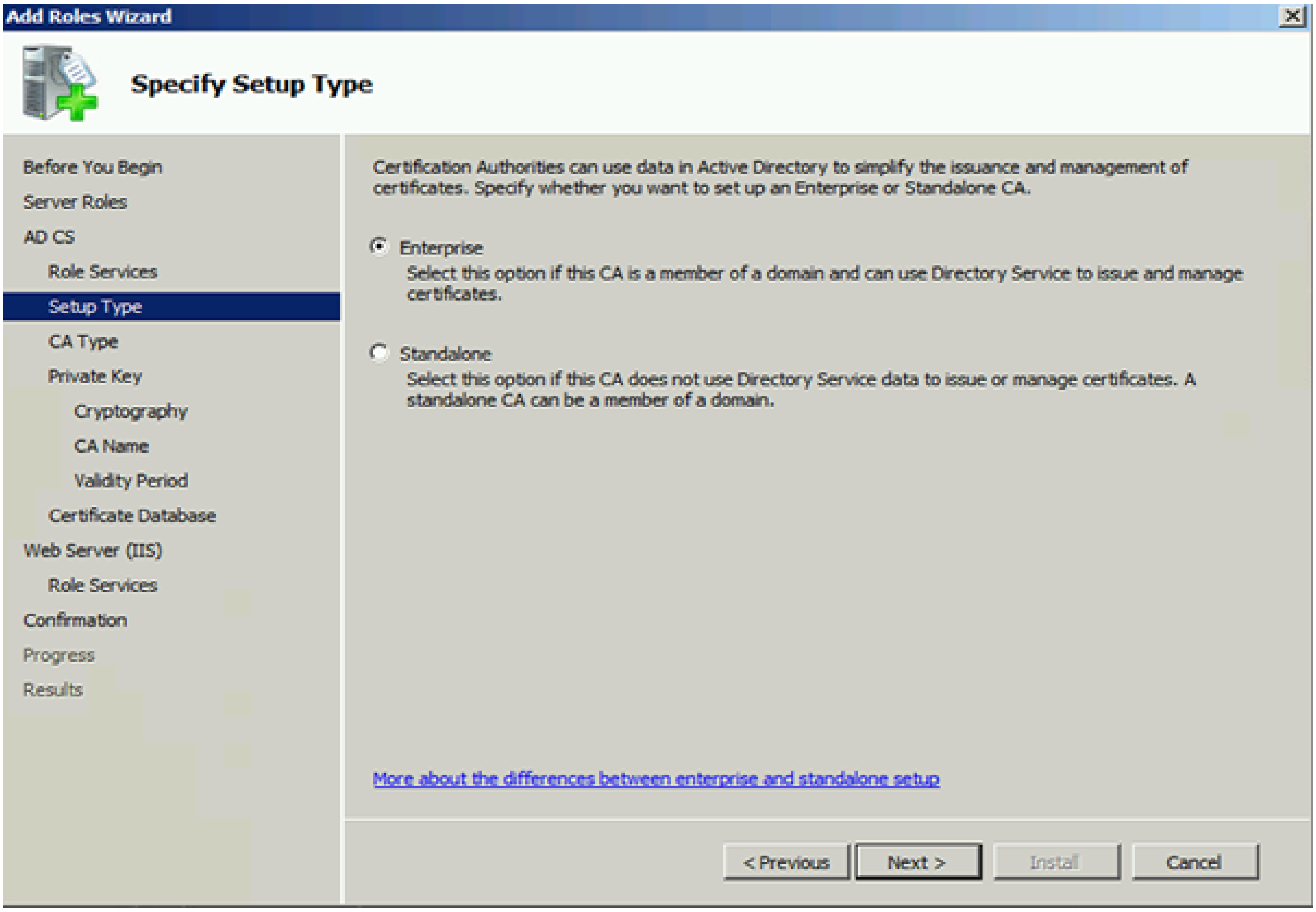
Description

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

さらに、これらのサービスを導入します。まず、Certificate Authority Certificate Enrollment Policy Web Serviceです。これら2つの役割をインストールした後、それらを設定し、**Certificate Enrollment Web ServiceとCertificate Authority Web Enrollmentをインストールします**。設定します。

IISなどの追加の役割サービスおよび機能は、証明機関のインストール時にも追加されます。

導入に応じて、[エンタープライズ(Enterprise)]または[スタンドアロン(Standalone)]を選択できます。



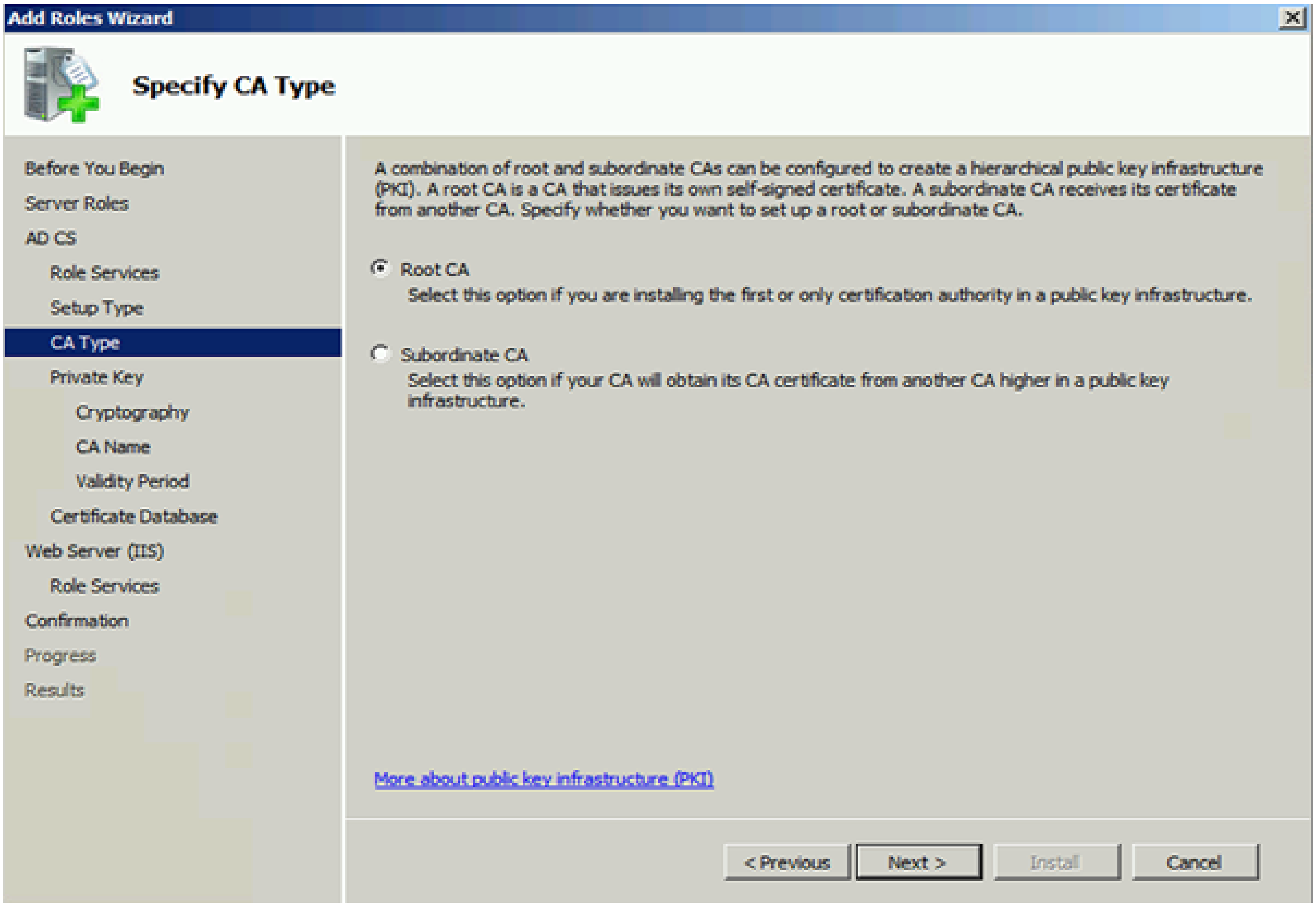
Certification Authorities can use data in Active Directory to simplify the issuance and management of certificates. Specify whether you want to set up an Enterprise or Standalone CA.

● Enterprise
Select this option if this CA is a member of a domain and can use Directory Service to issue and manage certificates.

○ Standalone
Select this option if this CA does not use Directory Service data to issue or manage certificates. A standalone CA can be a member of a domain.

More about the differences between enterprise and standalone setup

[CA Type]では、[Root CA]または[Subordinate CA]を選択できます。組織内で実行中のCAが他にない場合は、[ルートCA]を**選択します**。

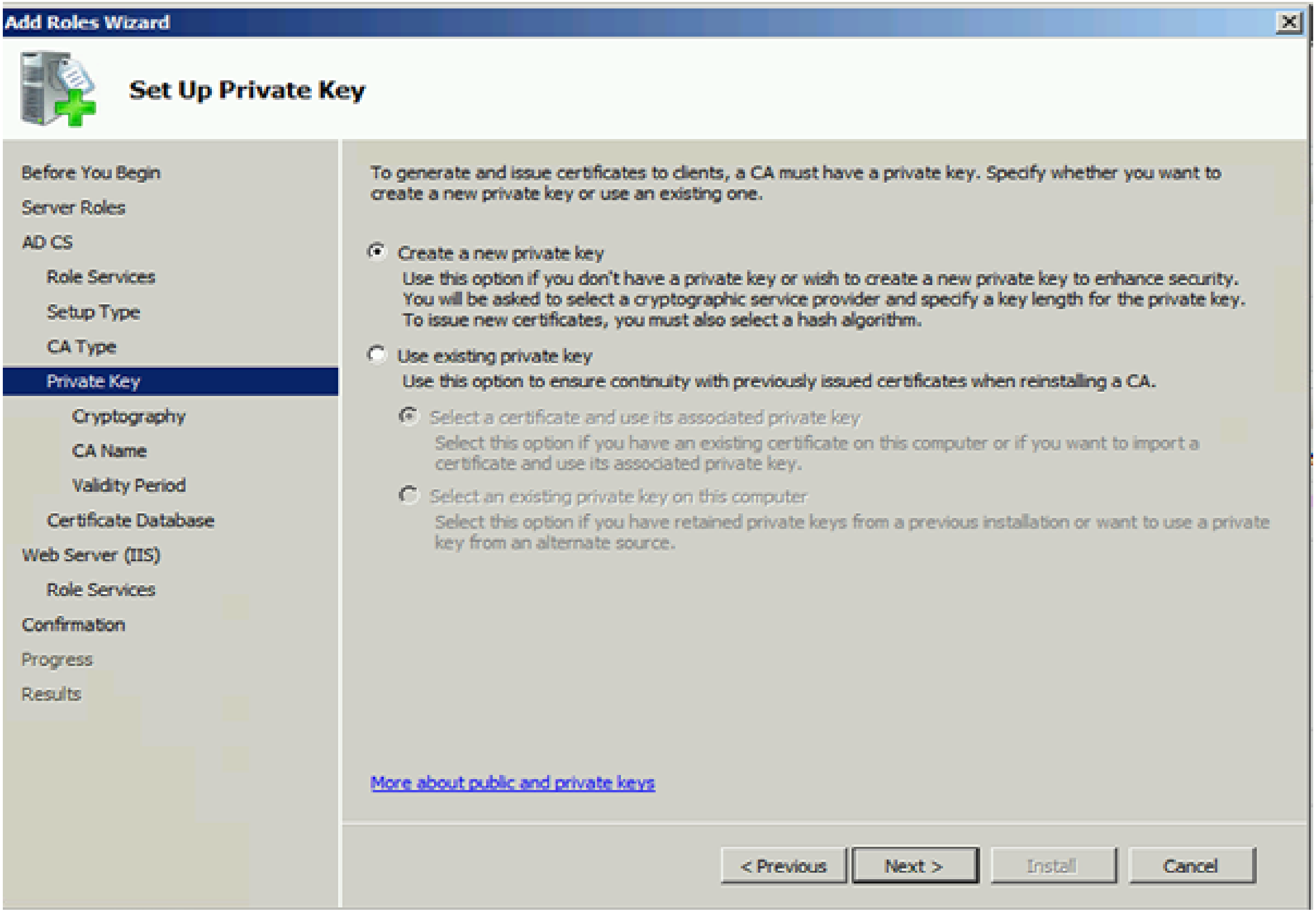


A combination of root and subordinate CAs can be configured to create a hierarchical public key infrastructure (PKI). A root CA is a CA that issues its own self-signed certificate. A subordinate CA receives its certificate from another CA. Specify whether you want to set up a root or subordinate CA.

● Root CA
Select this option if you are installing the first or only certification authority in a public key infrastructure.

○ Subordinate CA
Select this option if your CA will obtain its CA certificate from another CA higher in a public key infrastructure.

次に、CAの秘密キーを作成します。



To generate and issue certificates to clients, a CA must have a private key. Specify whether you want to create a new private key or use an existing one.

● Create a new private key
Use this option if you don't have a private key or wish to create a new private key to enhance security. You will be asked to select a cryptographic service provider and specify a key length for the private key. To issue new certificates, you must also select a hash algorithm.

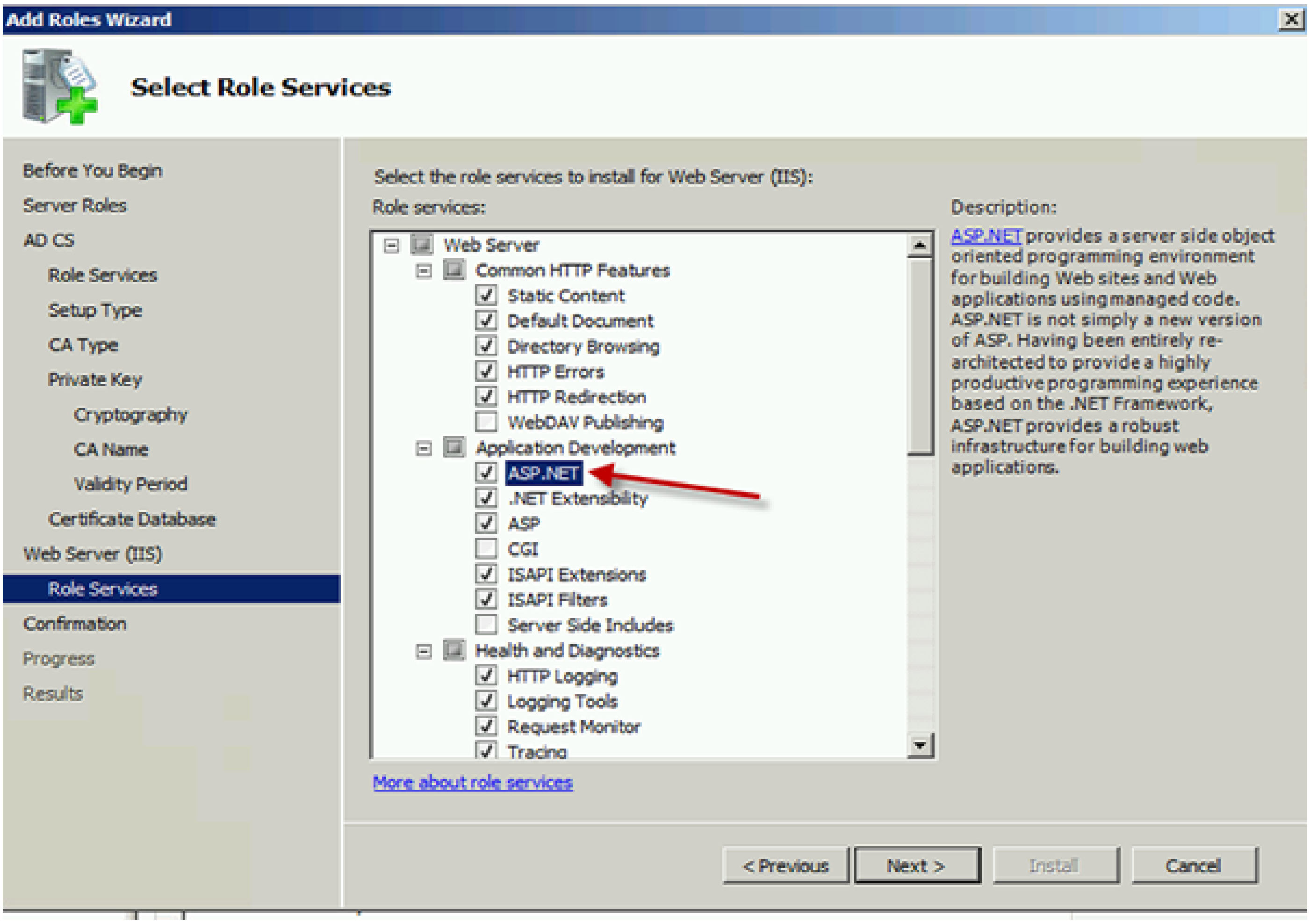
○ Use existing private key
Use this option to ensure continuity with previously issued certificates when reinstalling a CA.

● Select a certificate and use its associated private key
Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.

○ Select an existing private key on this computer
Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.

この手順は、ADFS3を別のWindows Server 2012にインストールする場合にのみ必要です。CAを

設定したら、IISの役割サービスを設定する必要があります。これは、CAでのWeb登録に必要です。ほとんどのADFSの展開では、IISに追加の役割が必要です。アプリケーション開発の下の**ASP.NET**をクリックしてください。



Add Roles Wizard

Select Role Services

Before You Begin
Server Roles
AD CS
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Web Server (IIS)
Role Services
Confirmation
Progress
Results

Select the role services to install for Web Server (IIS):

Role services:

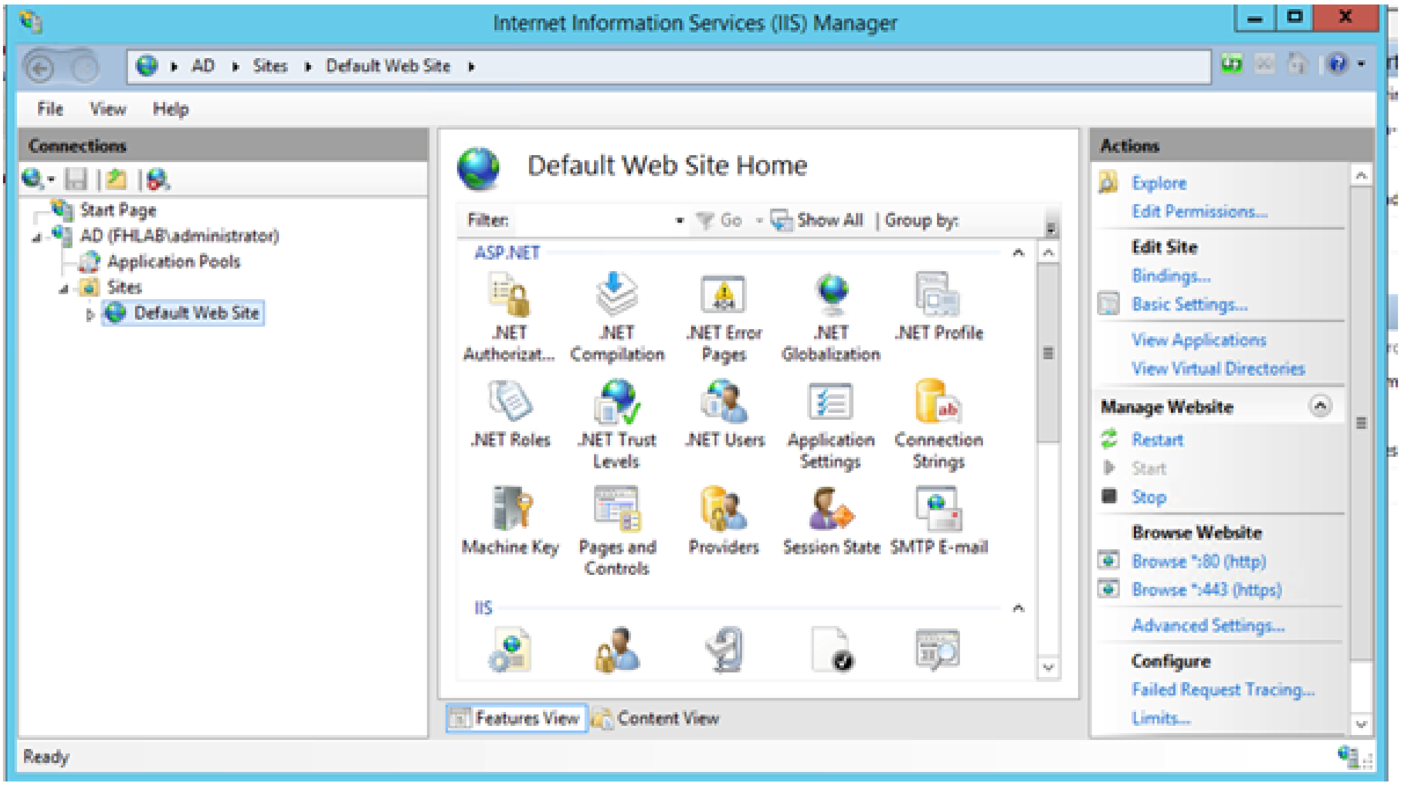
- Web Server
  - Common HTTP Features
    - ☑ Static Content
    - ☑ Default Document
    - ☑ Directory Browsing
    - ☑ HTTP Errors
    - ☑ HTTP Redirection
    - □ WebDAV Publishing
  - Application Development
    - ☑ ASP.NET
    - ☑ .NET Extensibility
    - ☑ ASP
    - □ CGI
    - ☑ ISAPI Extensions
    - ☑ ISAPI Filters
    - □ Server Side Includes
  - Health and Diagnostics
    - ☑ HTTP Logging
    - ☑ Logging Tools
    - ☑ Request Monitor
    - ☑ Tracing

Description:

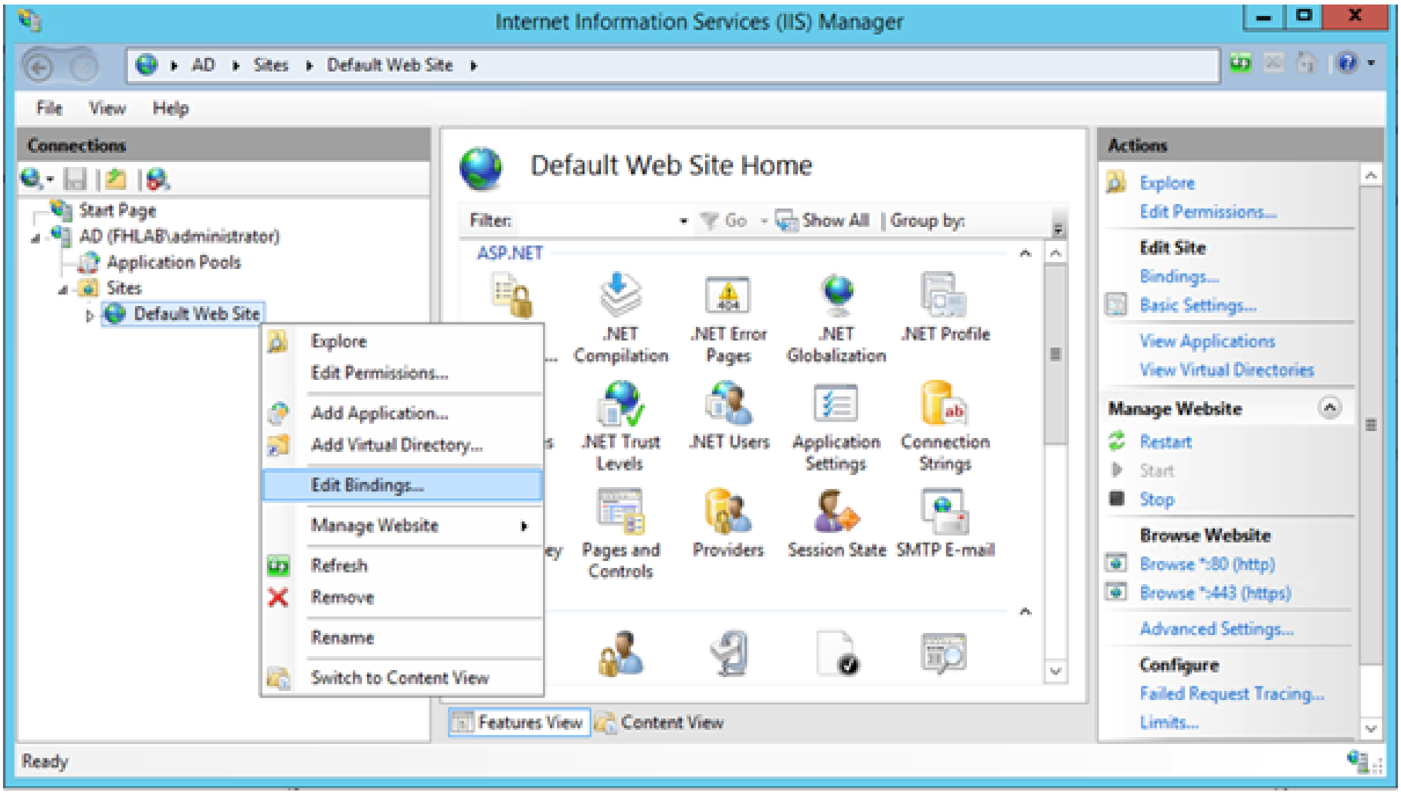
ASP.NET provides a server side object oriented programming environment for building Web sites and Web applications using managed code. ASP.NET is not simply a new version of ASP. Having been entirely re-architected to provide a highly productive programming experience based on the .NET Framework, ASP.NET provides a robust infrastructure for building web applications.

More about role services

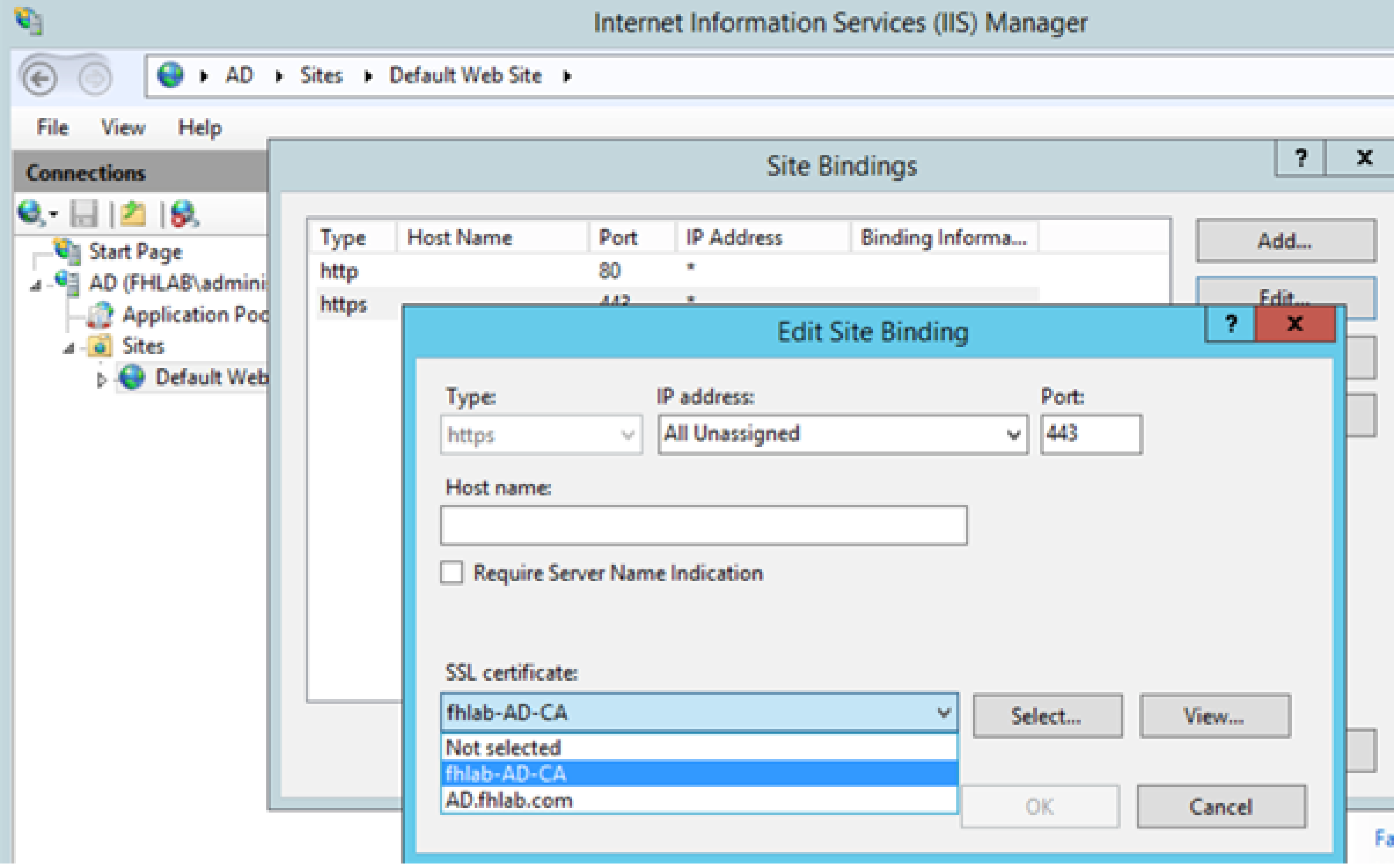
サーバーマネージャーで、[Webサー**バー] > [IIS]をクリック**し、[既定のWebサイト]を右クリ**ックします**。HTTPに加えてHTTPSを許可するようにバインドを変更する必要があります。これは、HTTPSをサポートするために行われます。



「バインディングの編集」を選択します。



新しいサイトバインドを追加し、タイプとしてHTTPSを選択します。SSL証明書で、ADサーバと同じFQDNを持つサーバ証明書を選択します。



Type	Host Name	Port	IP Address	Binding Informa...
http		80	*	
https		443	*	

Type: https

IP address: All Unassigned

Port: 443

Host name:

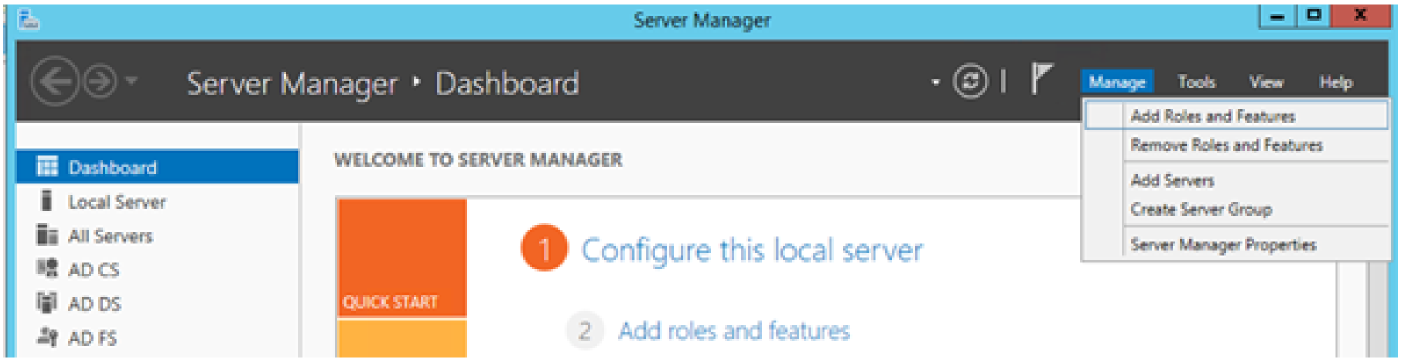
□ Require Server Name Indication

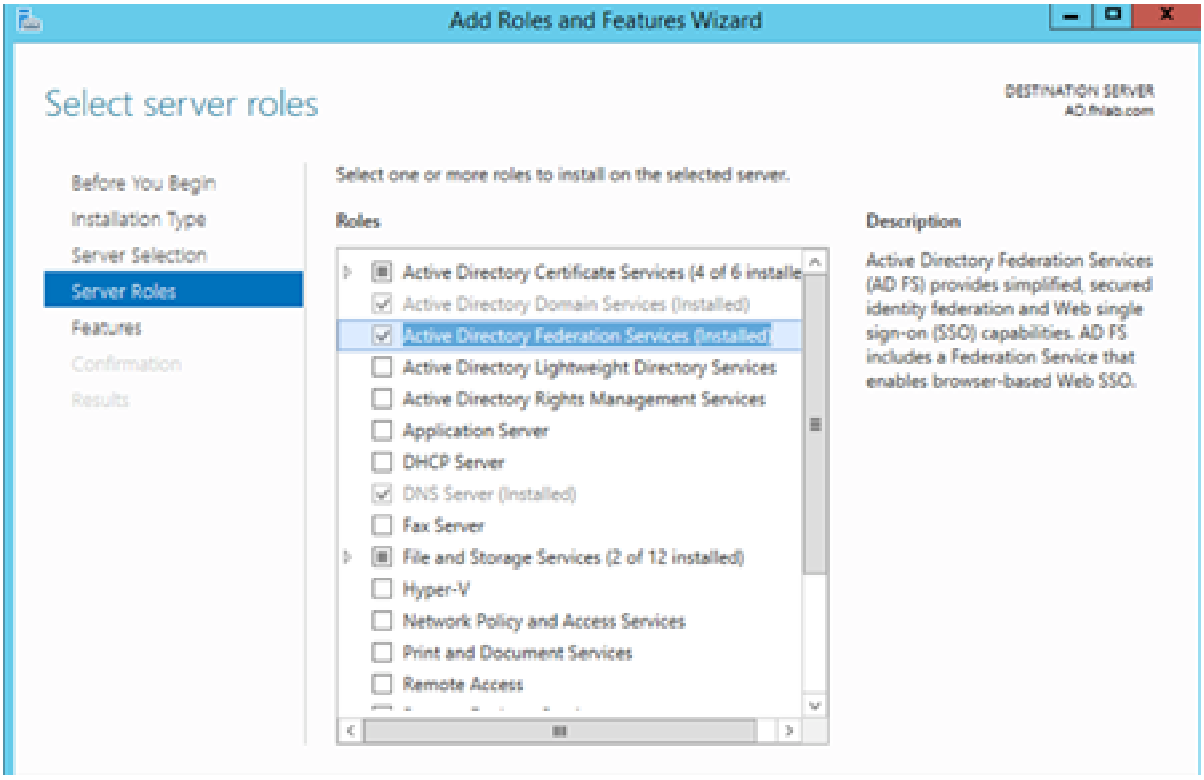
SSL certificate: fhlab-AD-CA

Not selected
fhlab-AD-CA
AD.fhlab.com

前提条件のすべての役割が環境にインストールされているため、ADFS3 Active Directoryフェデレーションサービス(Windows Server 2012)のインストールを続行できます。

サーバーの役割については、[サーバー**マネージャー] > [管理] > [サーバーの役割と機能の追加]に移動し**て、プライベートLAN上の顧客ネットワーク内に**IDPをインストールする**と、[Active Directoryフェデレーションサービス]を選択します。





Select one or more roles to install on the selected server.

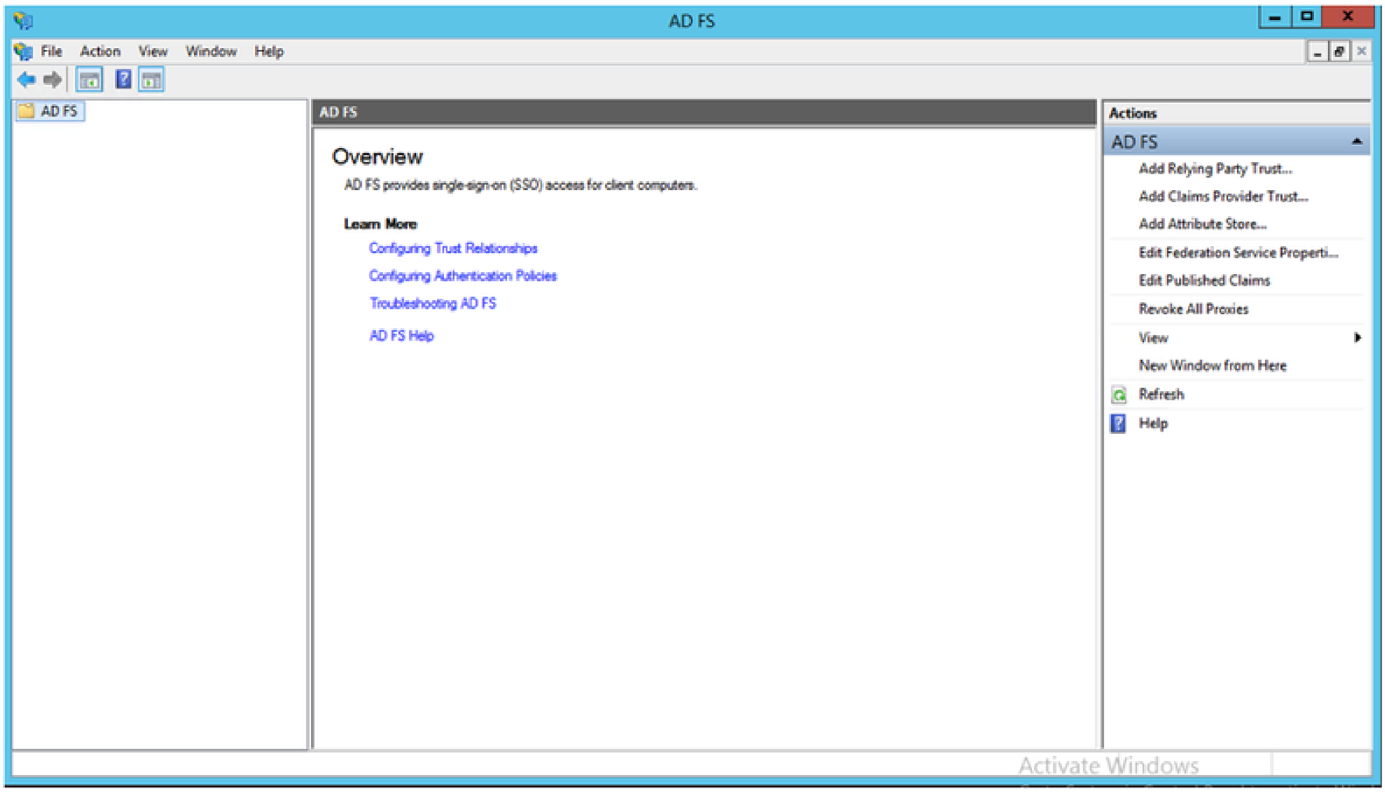
Roles

- ▣ Active Directory Certificate Services (4 of 6 installe
- ☑ Active Directory Domain Services (Installed)
- ☑ Active Directory Federation Services (Installed)
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☐ DHCP Server
- ☑ DNS Server (Installed)
- ☐ Fax Server
- ▣ File and Storage Services (2 of 12 installed)
- ☐ Hyper-V
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access

Description

Active Directory Federation Services (AD FS) provides simplified, secured identity federation and Web single sign-on (SSO) capabilities. AD FS includes a Federation Service that enables browser-based Web SSO.

インストールが完了したら、タスクバーまたは[スタート]メニューから開くことができます。



Overview

AD FS provides single-sign-on (SSO) access for client computers.

Learn More

Configuring Trust Relationships

Configuring Authentication Policies

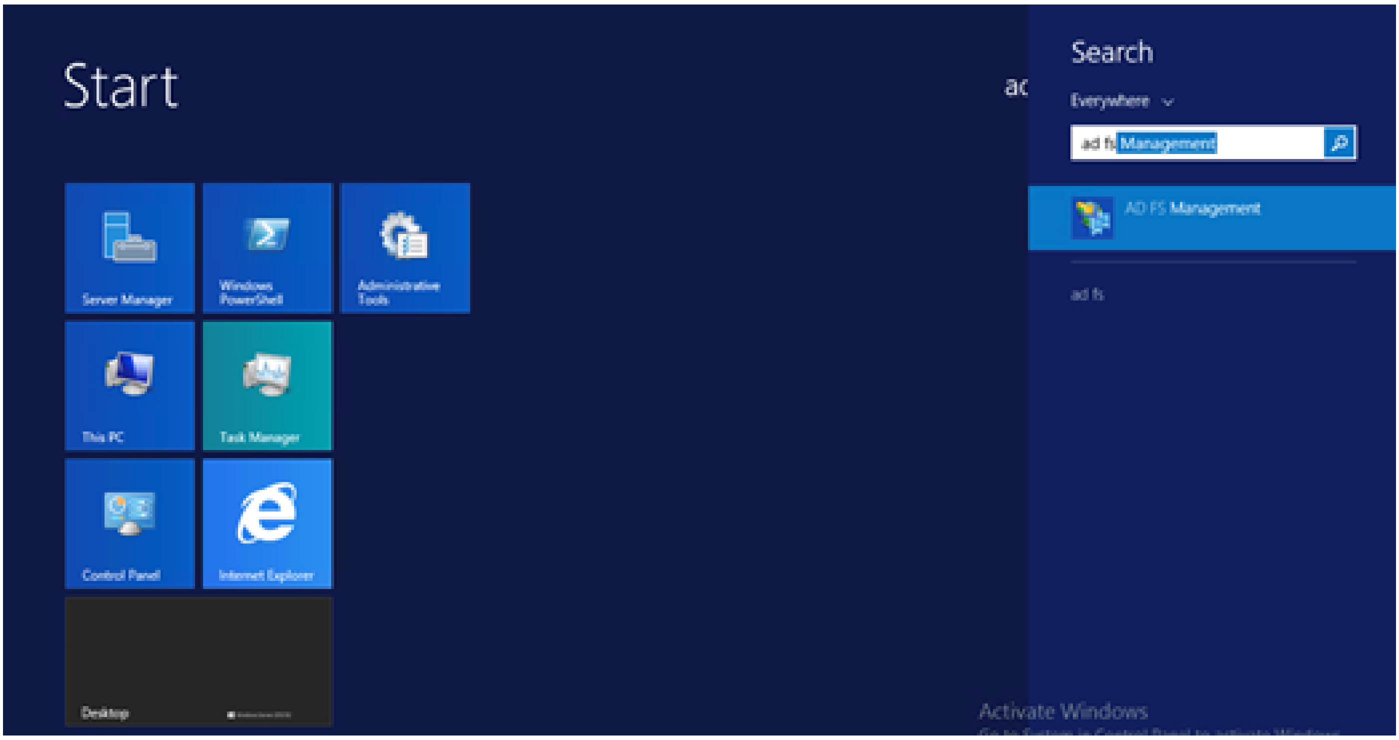
Troubleshooting AD FS

AD FS Help

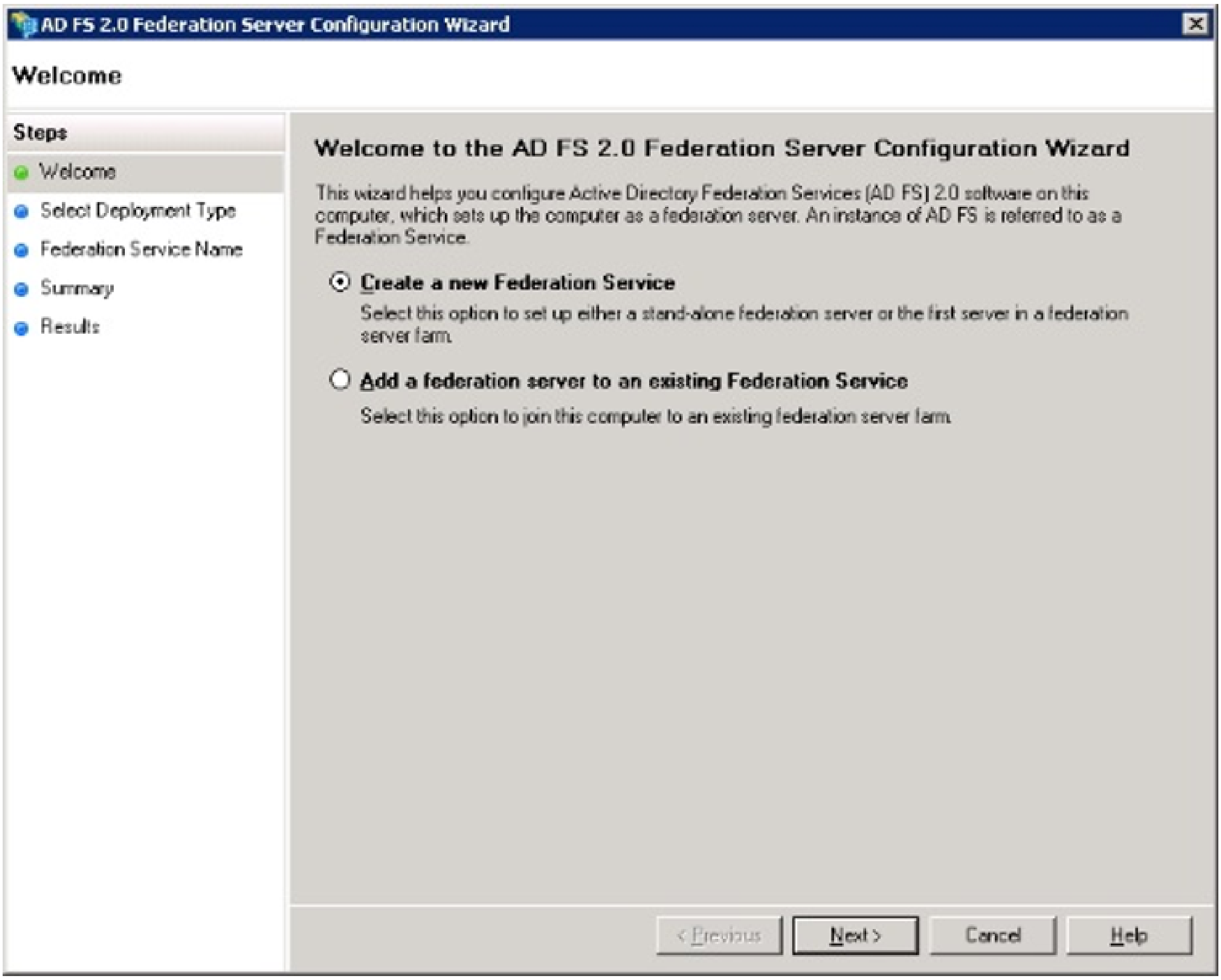
ADFS3の初期設定

このセクションでは、新しいスタンドアロンフェデレーションサーバのインストールについて説明しますが、ドメインコントローラにインストールする場合にも使用できます

図に示**すようにADFS**管理コンソールを起動するには、[Windows]を選択して、「AD FS Management」と入力します。



[AD FS 3.0 Federation Server Configuration Wizard]**オプションを選択**して、ADFSサーバの設定を開始します。これらのスクリーンショットは、AD FS 3の同じ手順を表しています。



AD FS 2.0 Federation Server Configuration Wizard

Welcome

Steps
- Welcome
- Select Deployment Type
- Federation Service Name
- Summary
- Results

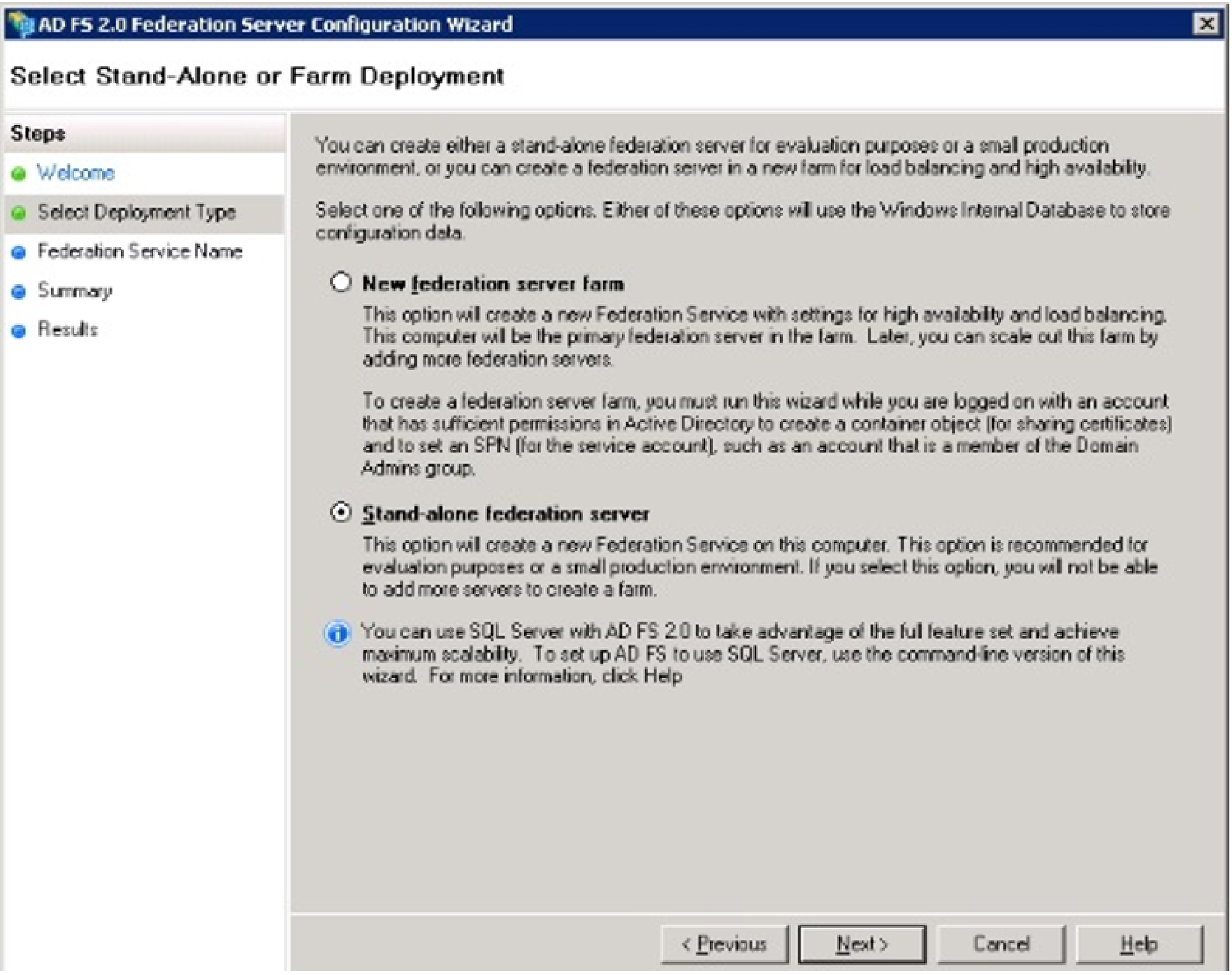
Welcome to the AD FS 2.0 Federation Server Configuration Wizard

This wizard helps you configure Active Directory Federation Services (AD FS) 2.0 software on this computer, which sets up the computer as a federation server. An instance of AD FS is referred to as a Federation Service.

● Create a new Federation Service
Select this option to set up either a stand-alone federation server or the first server in a federation server farm.

○ Add a federation server to an existing Federation Service
Select this option to join this computer to an existing federation server farm.

[新しいフェデレーションサービスを作**成する]を選択**し、[次へ]を**クリックします。**



AD FS 2.0 Federation Server Configuration Wizard

Select Stand-Alone or Farm Deployment

You can create either a stand-alone federation server for evaluation purposes or a small production environment, or you can create a federation server in a new farm for load balancing and high availability.

Select one of the following options. Either of these options will use the Windows Internal Database to store configuration data.

○ New federation server farm

This option will create a new Federation Service with settings for high availability and load balancing. This computer will be the primary federation server in the farm. Later, you can scale out this farm by adding more federation servers.

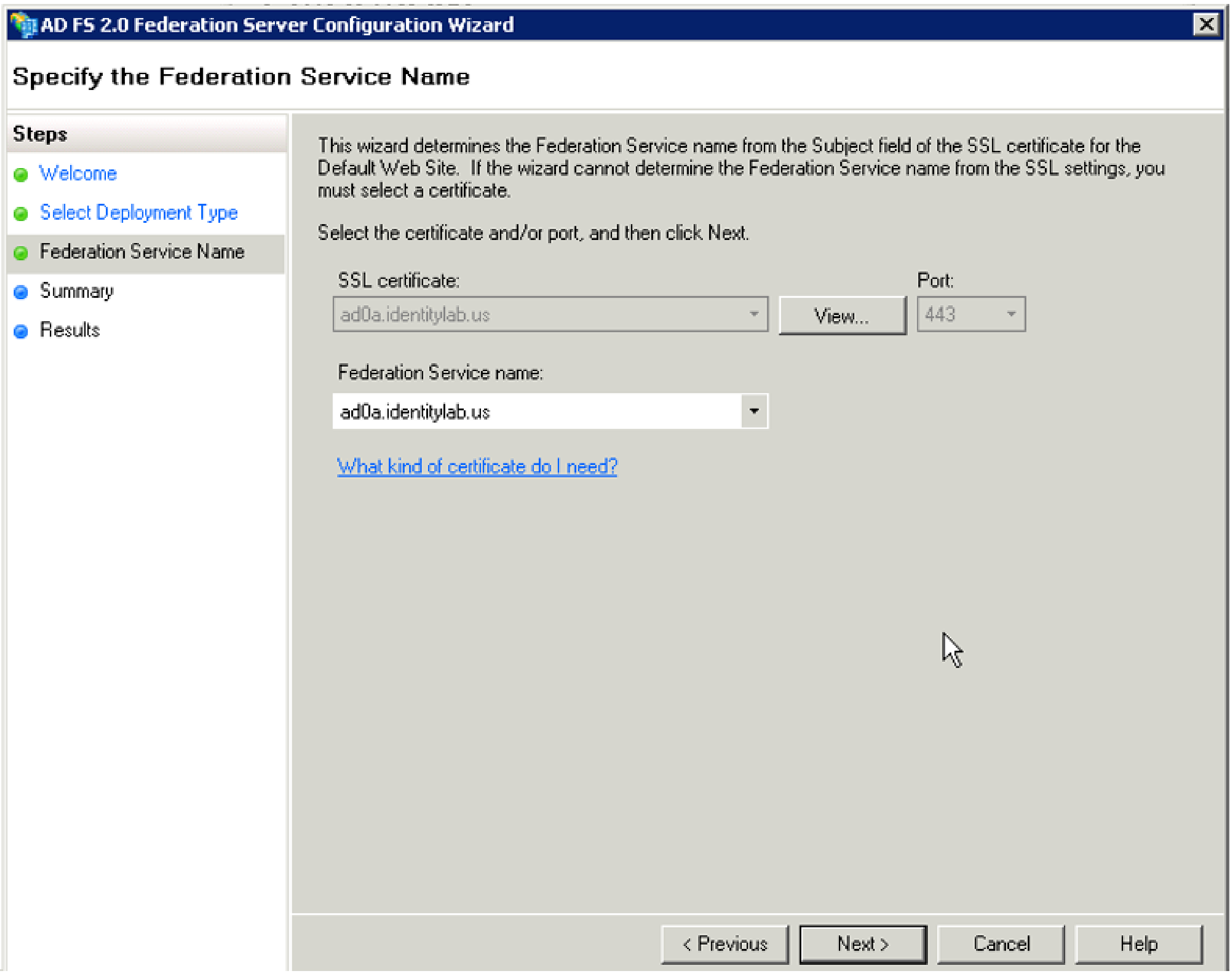
To create a federation server farm, you must run this wizard while you are logged on with an account that has sufficient permissions in Active Directory to create a container object (for sharing certificates) and to set an SPN (for the service account), such as an account that is a member of the Domain Admins group.

● Stand-alone federation server

This option will create a new Federation Service on this computer. This option is recommended for evaluation purposes or a small production environment. If you select this option, you will not be able to add more servers to create a farm.

You can use SQL Server with AD FS 2.0 to take advantage of the full feature set and achieve maximum scalability. To set up AD FS to use SQL Server, use the command-line version of this wizard. For more information, click Help

図に示すように、[スタンドアロンフェデレーションサーバ]を選択し、[次へ]をクリックします。



AD FS 2.0 Federation Server Configuration Wizard

Specify the Federation Service Name

This wizard determines the Federation Service name from the Subject field of the SSL certificate for the Default Web Site. If the wizard cannot determine the Federation Service name from the SSL settings, you must select a certificate.

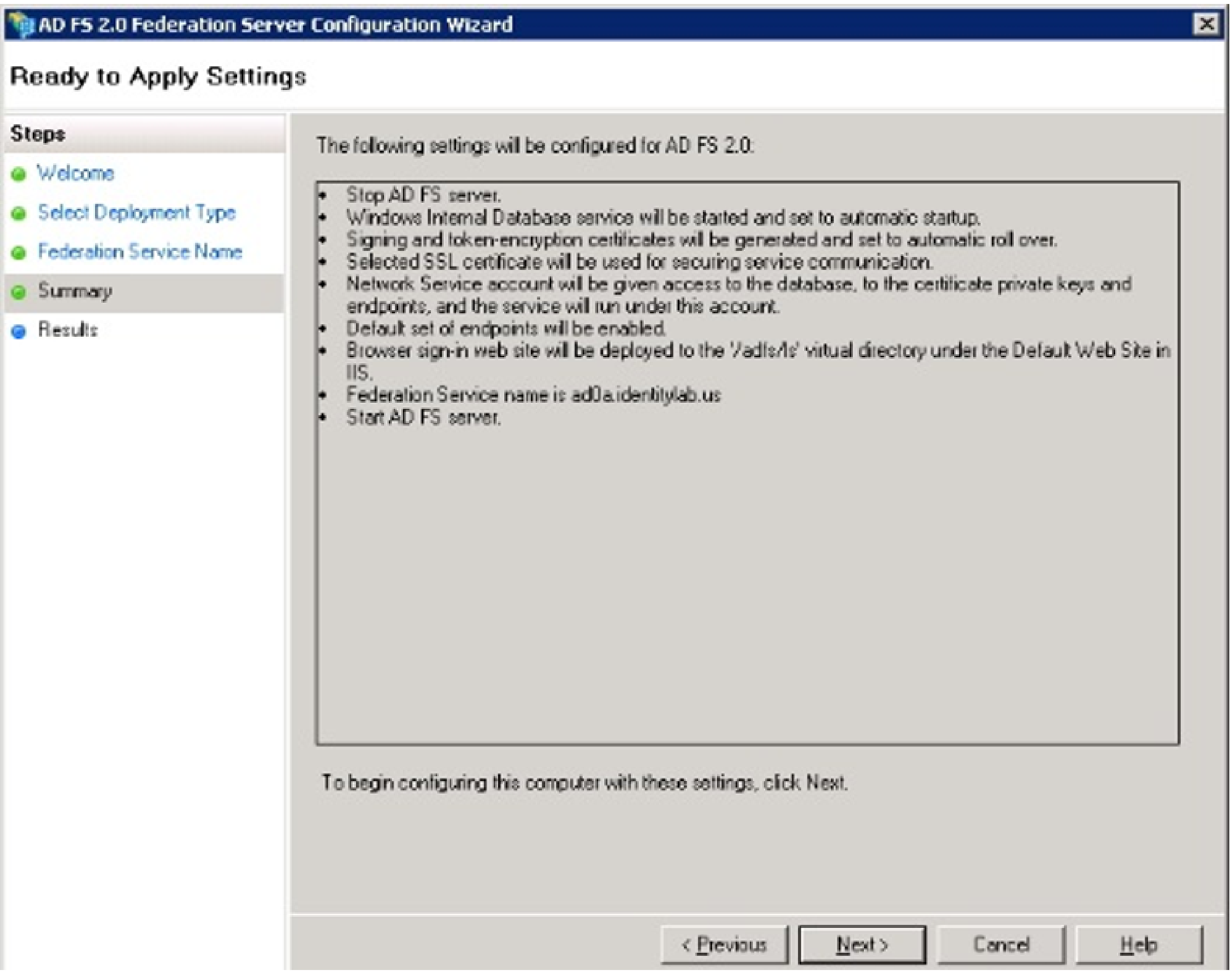
Select the certificate and/or port, and then click Next.

SSL certificate: ad0a.identitylab.us

Port: 443

Federation Service name: ad0a.identitylab.us

[SSL certificate]で、リストから自己署名証明書を選択します。フェデレーションサービス名が自動的に入力されます。[next] をクリックします。



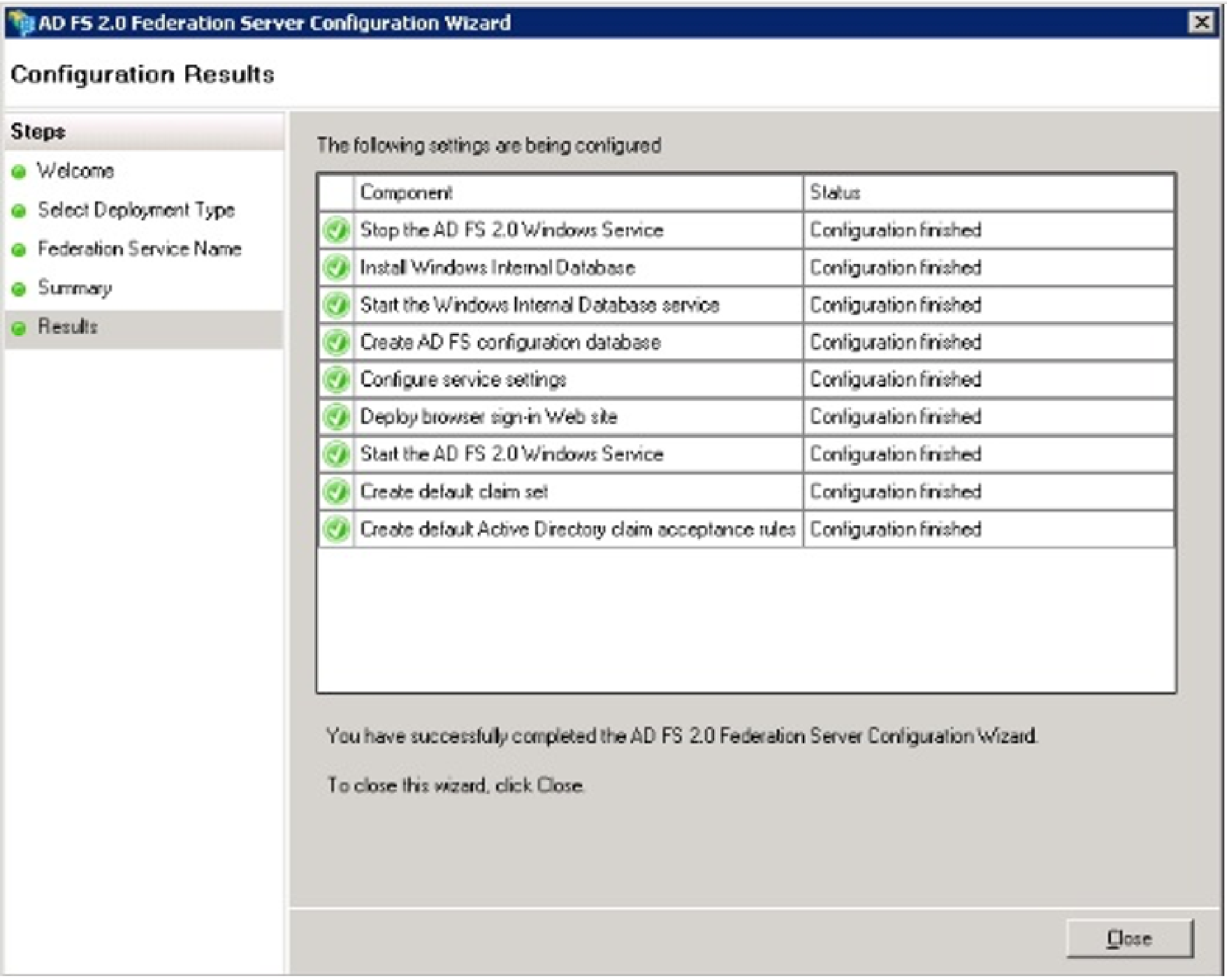
Ready to Apply Settings

The following settings will be configured for AD FS 2.0:

- Stop AD FS server.
- Windows Internal Database service will be started and set to automatic startup.
- Signing and token-encryption certificates will be generated and set to automatic roll over.
- Selected SSL certificate will be used for securing service communication.
- Network Service account will be given access to the database, to the certificate private keys and endpoints, and the service will run under this account.
- Default set of endpoints will be enabled.
- Browser sign-in web site will be deployed to the '/adfs/ls' virtual directory under the Default Web Site in IIS.
- Federation Service name is ad0a.identitylab.us
- Start AD FS server.

To begin configuring this computer with these settings, click Next.

設定を確認し、[Next]をクリックして設定を適用します。



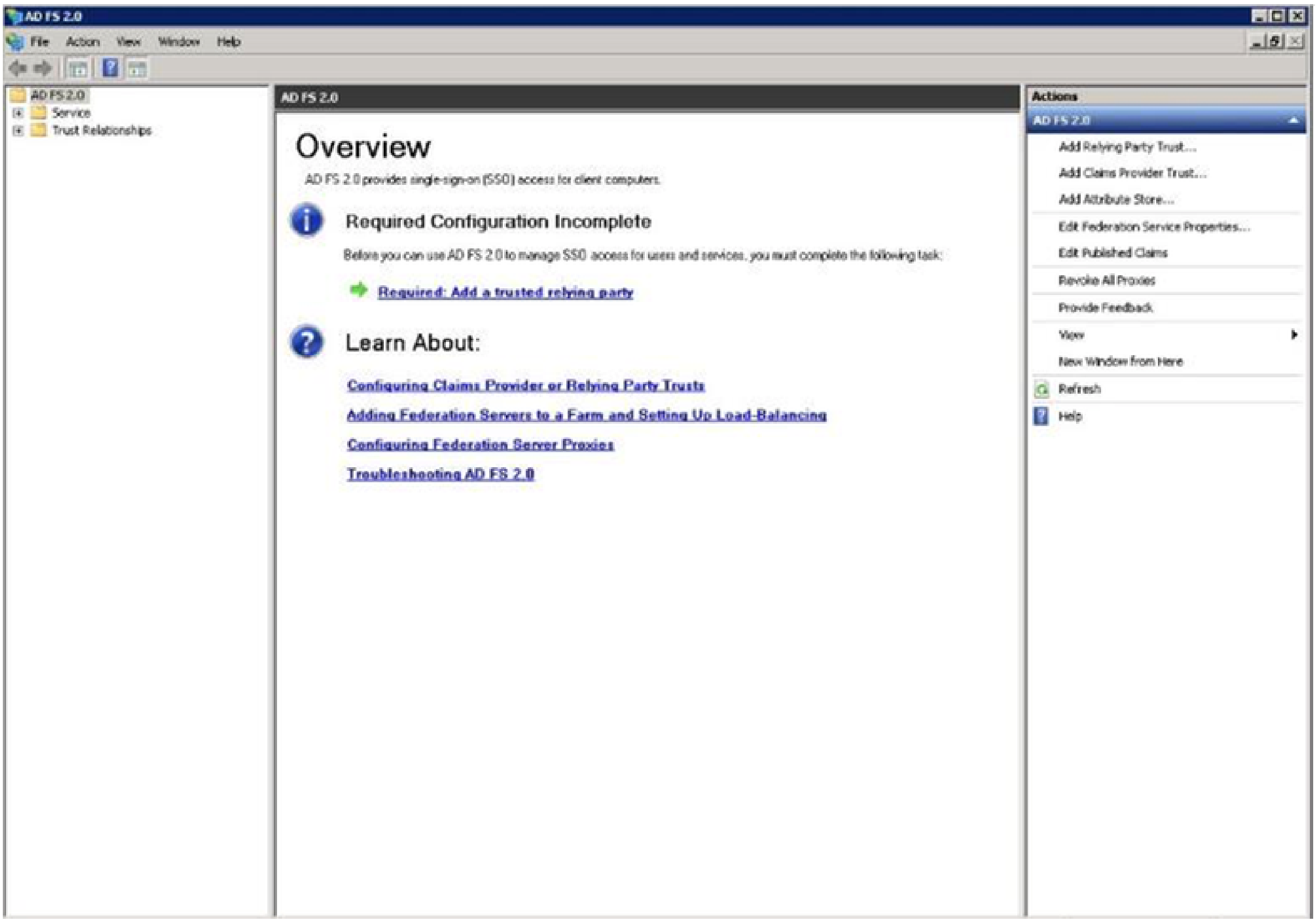
The following settings are being configured

	Component	Status
✓	Stop the AD FS 2.0 Windows Service	Configuration finished
✓	Install Windows Internal Database	Configuration finished
✓	Start the Windows Internal Database service	Configuration finished
✓	Create AD FS configuration database	Configuration finished
✓	Configure service settings	Configuration finished
✓	Deploy browser sign-in Web site	Configuration finished
✓	Start the AD FS 2.0 Windows Service	Configuration finished
✓	Create default claim set	Configuration finished
✓	Create default Active Directory claim acceptance rules	Configuration finished

You have successfully completed the AD FS 2.0 Federation Server Configuration Wizard.

To close this wizard, click Close.

すべてのコンポーネントが正常に完了したことを確認し、[Close]をクリックしてウィザードを終了し、メイン管理コンソールに戻ります。これには数分かかることがあります。



Overview

AD FS 2.0 provides single-sign-on (SSO) access for client computers.

Required Configuration Incomplete

Before you can use AD FS 2.0 to manage SSO access for users and services, you must complete the following task:

Required: Add a trusted relying party

Learn About:

Configuring Claims Provider or Relying Party Trusts

Adding Federation Servers to a Farm and Setting Up Load-Balancing

Configuring Federation Server Proxies

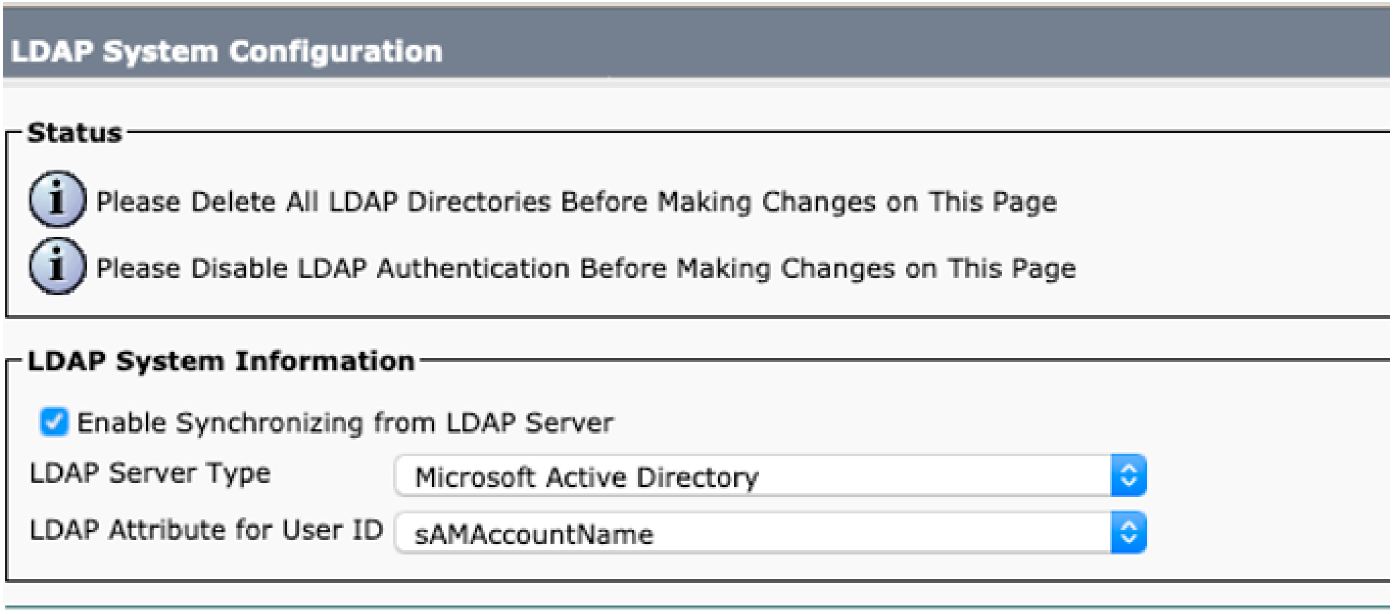
Troubleshooting AD FS 2.0

ADFSが有効になり、アイデンティティプロバイダー(IdP)として設定されるようになりました。次に、信頼できる証明書利用者としてCUCMを追加する必要があります。これを行う前に、まずCUCM Administrationで設定を行う必要があります。

ADFSを使用したCUCMでのSSOの設定

LDAP設定

クラスタはActive DirectoryとLDAP統合する必要があり、さらに先に進む前にLDAP認証を設定する必要があります。図に示すように、**[System]タブ> [LDAP System]**に移動します。



LDAP System Configuration

Status

Please Delete All LDAP Directories Before Making Changes on This Page

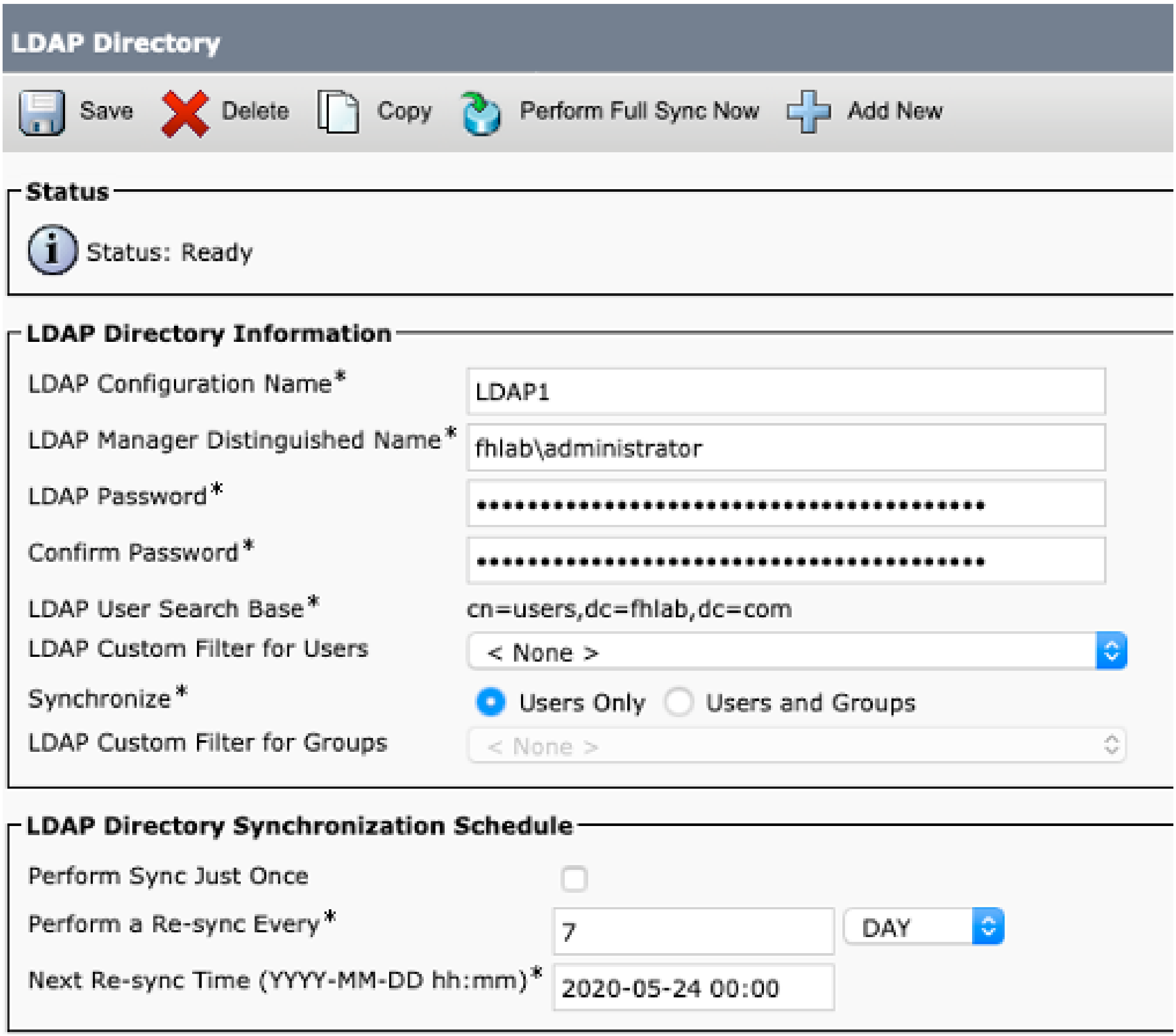
Please Disable LDAP Authentication Before Making Changes on This Page

LDAP System Information

☑ Enable Synchronizing from LDAP Server

LDAP Server Type	Microsoft Active Directory
LDAP Attribute for User ID	sAMAccountName

次に、[システム]タブ> **[LDAPディレクトリ]に移動します。**



LDAP Directory

Status

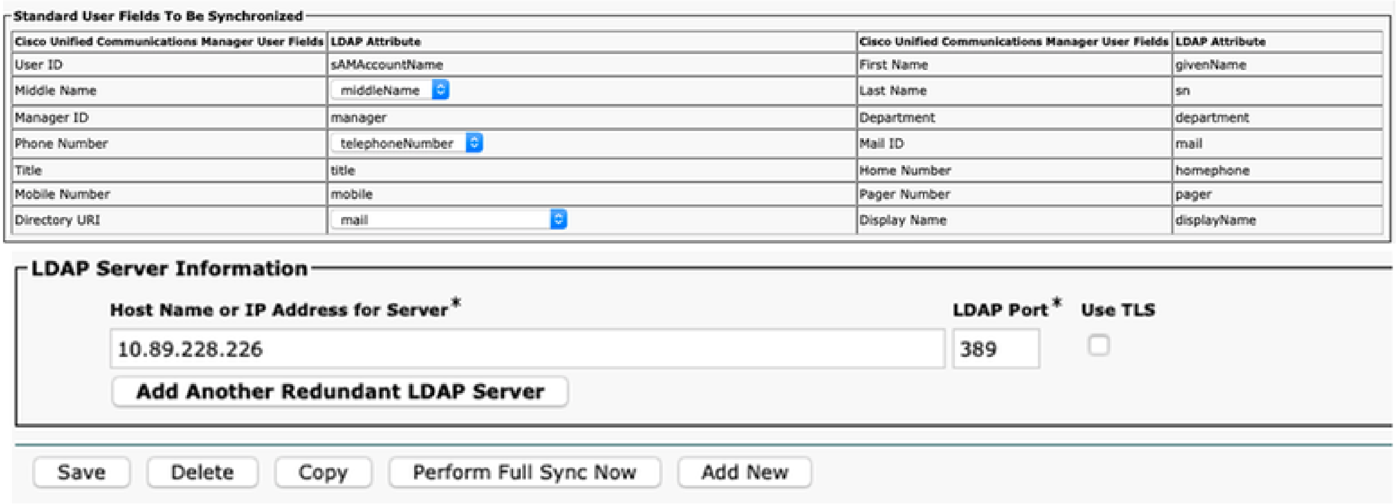
Status: Ready

LDAP Directory Information

LDAP Configuration Name*	LDAP1
LDAP Manager Distinguished Name*	fhlab\administrator
LDAP Password*	•••
Confirm Password*	•••
LDAP User Search Base*	cn=users,dc=fhlab,dc=com
LDAP Custom Filter for Users	< None >
Synchronize*	● Users Only ○ Users and Groups
LDAP Custom Filter for Groups	< None >

LDAP Directory Synchronization Schedule

Perform Sync Just Once	□
Perform a Re-sync Every*	7 DAY
Next Re-sync Time (YYYY-MM-DD hh:mm)*	2020-05-24 00:00



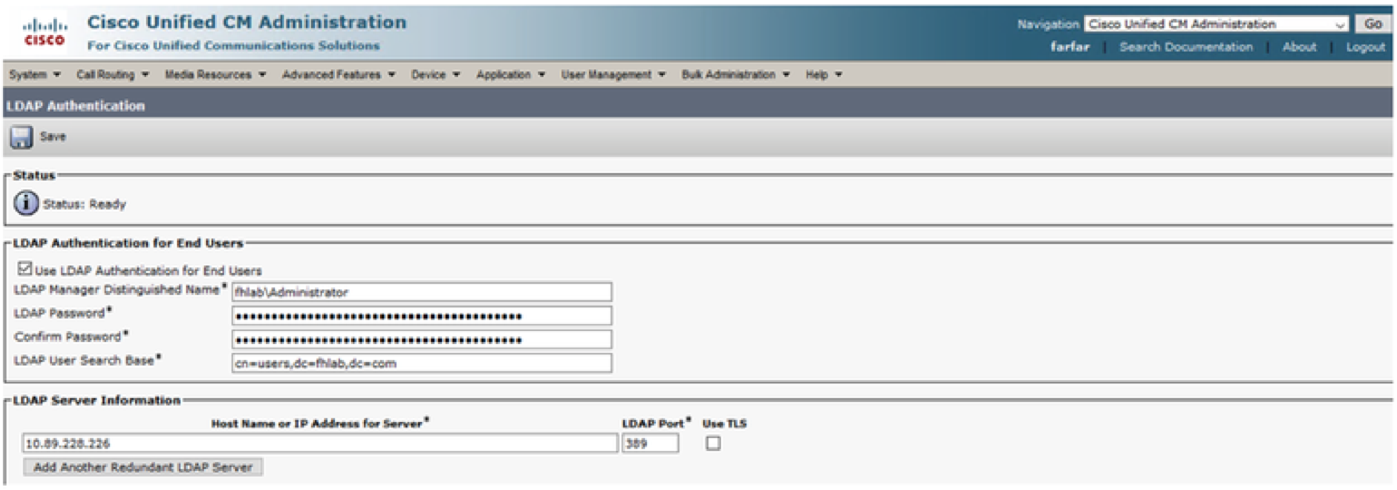
Standard User Fields To Be Synchronized

Cisco Unified Communications Manager User Fields	LDAP Attribute	Cisco Unified Communications Manager User Fields	LDAP Attribute
User ID	sAMAccountName	First Name	givenName
Middle Name	middleName	Last Name	sn
Manager ID	manager	Department	department
Phone Number	telephoneNumber	Mail ID	mail
Title	title	Home Number	homephone
Mobile Number	mobile	Pager Number	pager
Directory URI	mail	Display Name	displayName

LDAP Server Information

Host Name or IP Address for Server*	LDAP Port*	Use TLS
10.89.228.226	389	□

Active DirectoryユーザをCUCMと同期した後、LDAP認証を設定する必要があります。



Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration
Go
farfar | Search Documentation | About | Logout
System
Call Routing
Media Resources
Advanced Features
Device
Application
User Management
Bulk Administration
Help
LDAP Authentication
Save

Status

Status: Ready

LDAP Authentication for End Users

☑ Use LDAP Authentication for End Users

LDAP Manager Distinguished Name* fhlab\Administrator

LDAP Password* ••

Confirm Password* ••

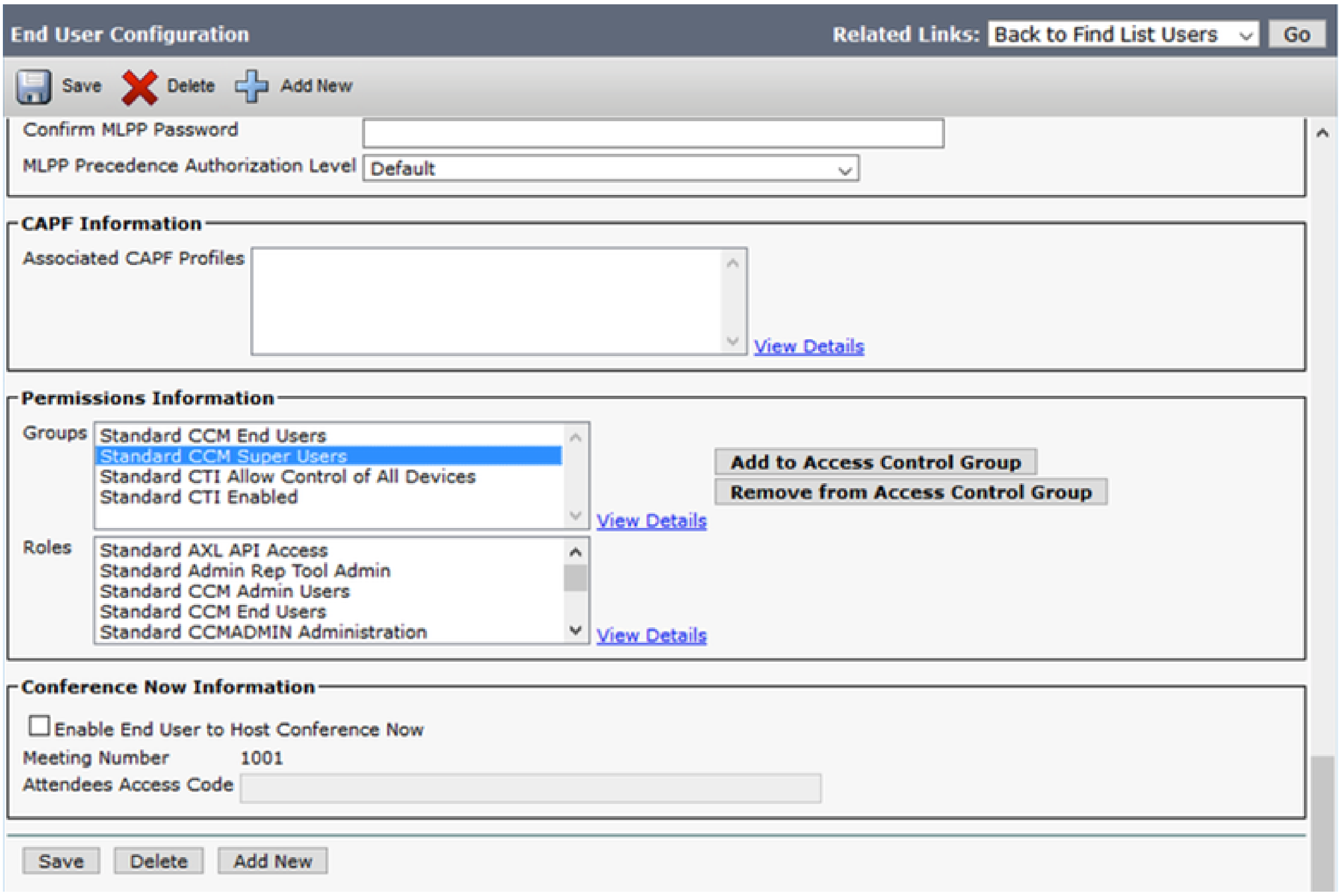
LDAP User Search Base* cn=users,dc=fhlab,dc=com

LDAP Server Information

Host Name or IP Address for Server*	LDAP Port*	Use TLS
10.89.228.226	389	□

Add Another Redundant LDAP Server

CUCMのエンドユーザは、特定のアクセスコントロールグループを自分のエンドユーザプロファイルに割り当てる必要があります。ACGは標準CCMスーパーユーザです。ユーザは、環境の準備ができたらSSOをテストするために使用されます。



End User Configuration
Related Links: Back to Find List Users
Go
Save
Delete
Add New

Confirm MLPP Password

MLPP Precedence Authorization Level: Default

CAPF Information

Associated CAPF Profiles

Permissions Information

Groups: Standard CCM End Users, Standard CCM Super Users, Standard CTI Allow Control of All Devices, Standard CTI Enabled

Add to Access Control Group
Remove from Access Control Group
View Details

Roles: Standard AXL API Access, Standard Admin Rep Tool Admin, Standard CCM Admin Users, Standard CCM End Users, Standard CCMADMIN Administration

Conference Now Information

□ Enable End User to Host Conference Now

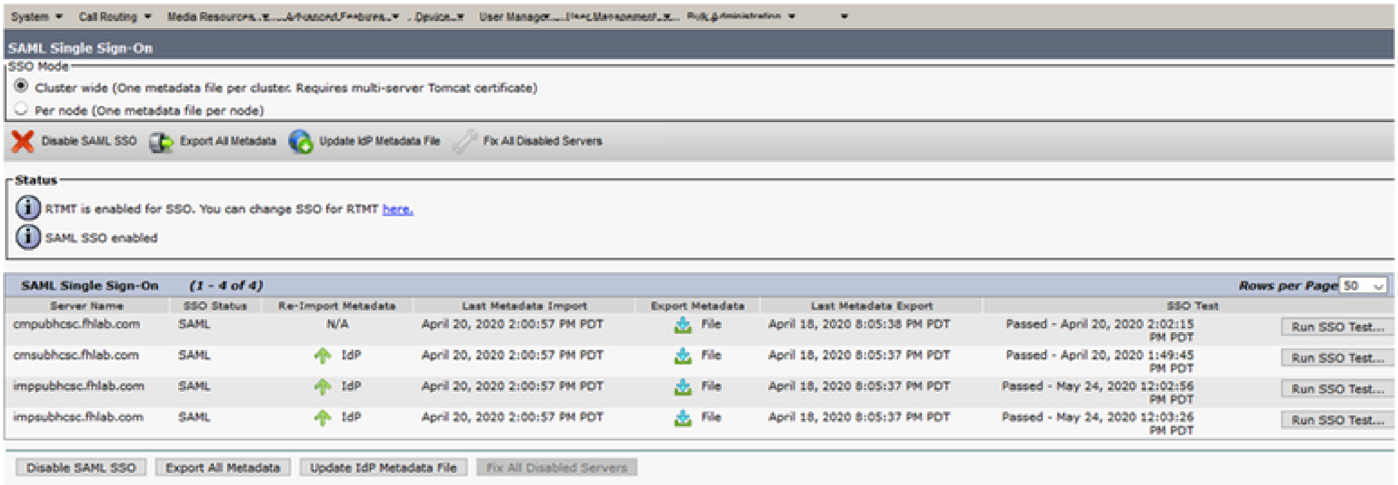
Meeting Number: 1001

Attendees Access Code

CUCMメタデータ

このセクションでは、CUCMパブリッシャのプロセスを示します。

最初の作業は、URLを参照する必要があるCUCMメタデータを取得することです。**https://<CUCM Pub FQDN>:8443/ssosp/ws/config/metadata/spをダウンロードする**か、**[System]タブ> [SAML Single Sign-on]からダウンロードできます。**これは、ノードまたはクラスタ全体ごとに実行できます。このクラスタ全体を実行することをお勧めします。



SSO Mode

● Cluster wide (One metadata file per cluster. Requires multi-server Tomcat certificate)

○ Per node (One metadata file per node)

Status

RTMT is enabled for SSO. You can change SSO for RTMT here.

SAML SSO enabled

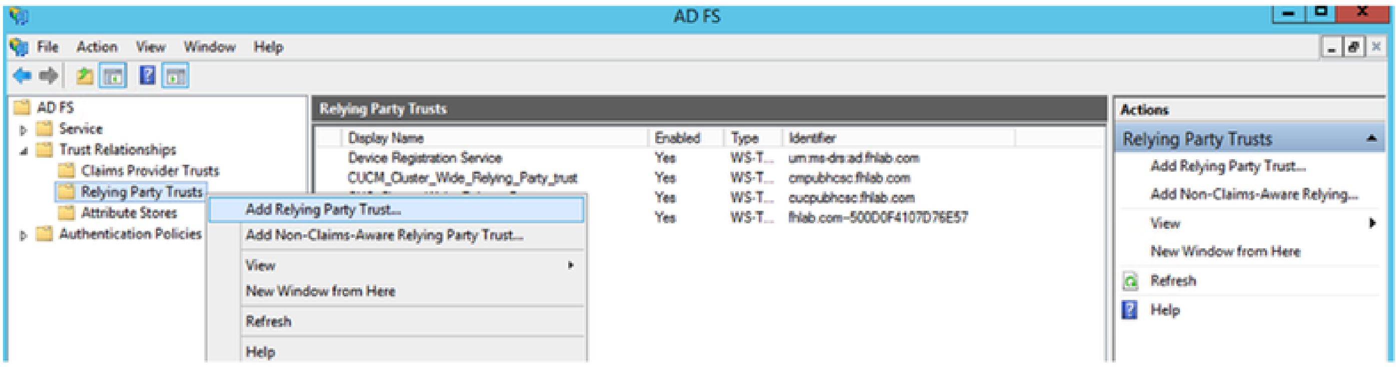
SAML Single Sign-On (1 - 4 of 4) Rows per Page 50

Server Name	SSO Status	Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	SSO Test	
cmpubhcsc.fhlab.com	SAML	N/A	April 20, 2020 2:00:57 PM PDT	File	April 18, 2020 8:05:38 PM PDT	Passed - April 20, 2020 2:02:15 PM PDT	Run SSO Test...
cmsubhcsc.fhlab.com	SAML	IdP	April 20, 2020 2:00:57 PM PDT	File	April 18, 2020 8:05:37 PM PDT	Passed - April 20, 2020 1:49:45 PM PDT	Run SSO Test...
imppubhcsc.fhlab.com	SAML	IdP	April 20, 2020 2:00:57 PM PDT	File	April 18, 2020 8:05:37 PM PDT	Passed - May 24, 2020 12:02:56 PM PDT	Run SSO Test...
impsubhcsc.fhlab.com	SAML	IdP	April 20, 2020 2:00:57 PM PDT	File	April 18, 2020 8:05:37 PM PDT	Passed - May 24, 2020 12:03:26 PM PDT	Run SSO Test...

sp_cucm0a.xmlなどの意味のある名前でデータをローカルに保存します。後で必要になります。

ADFS証明書利用者の設定

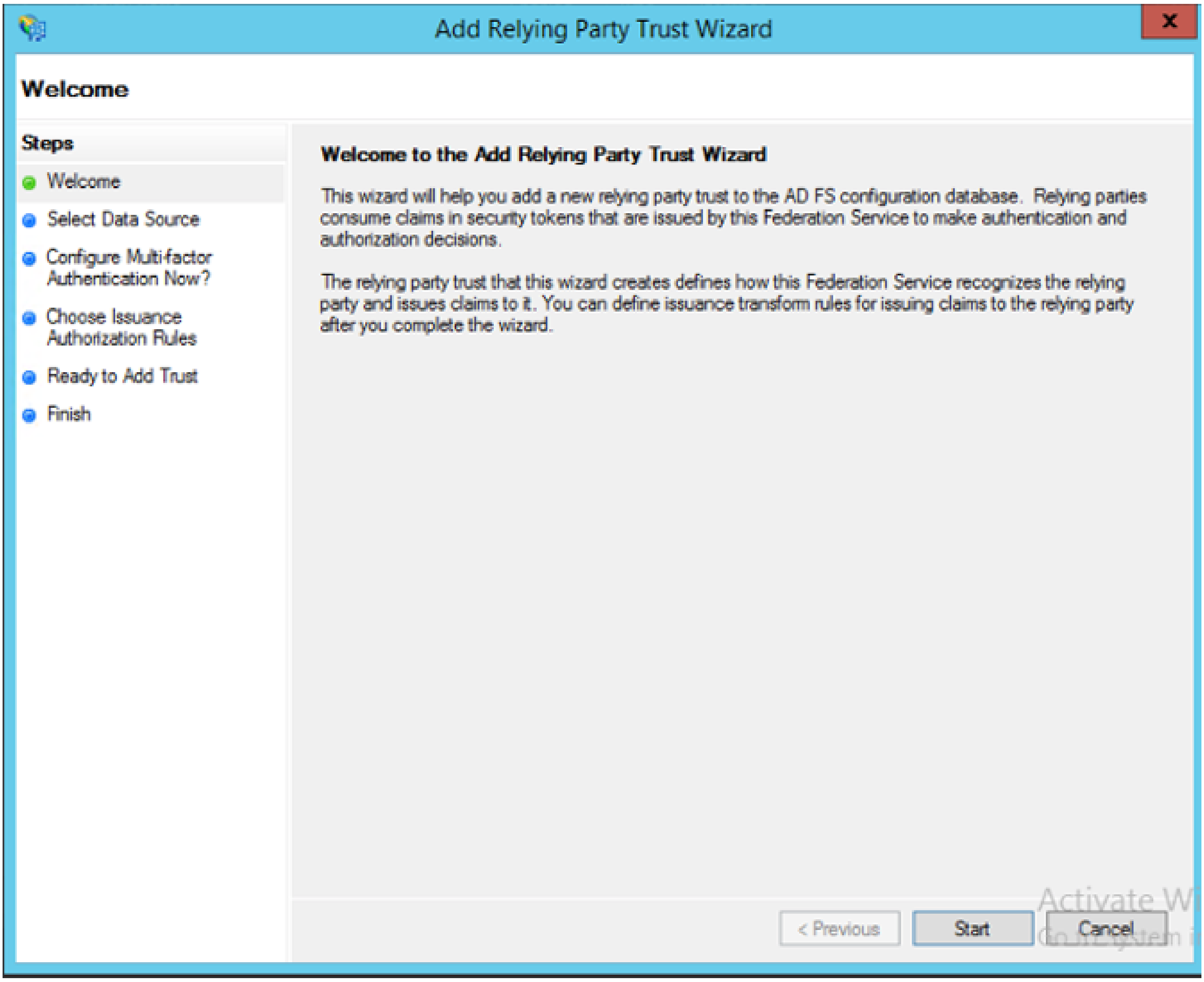
AD FS 3.0管理コンソールに戻ります。



Relying Party Trusts

Display Name	Enabled	Type	Identifier
Device Registration Service	Yes	WS-T...	urn:ms-drs:ad.fhlab.com
CUCM_Cluster_Wide_Relying_Party_trust	Yes	WS-T...	cmpubhcsc.fhlab.com
	Yes	WS-T...	cucpubhcsc.fhlab.com
	Yes	WS-T...	fhlab.com-500D0F4107D76E57

[Add Relying Party Trust Wizard]をクリックします。


Add Relying Party Trust Wizard
Steps
Welcome
Select Data Source
Configure Multi-factor Authentication Now?
Choose Issuance Authorization Rules
Ready to Add Trust
Finish
< Previous
Start
Cancel
Activate Wi
Go to System i

Welcome

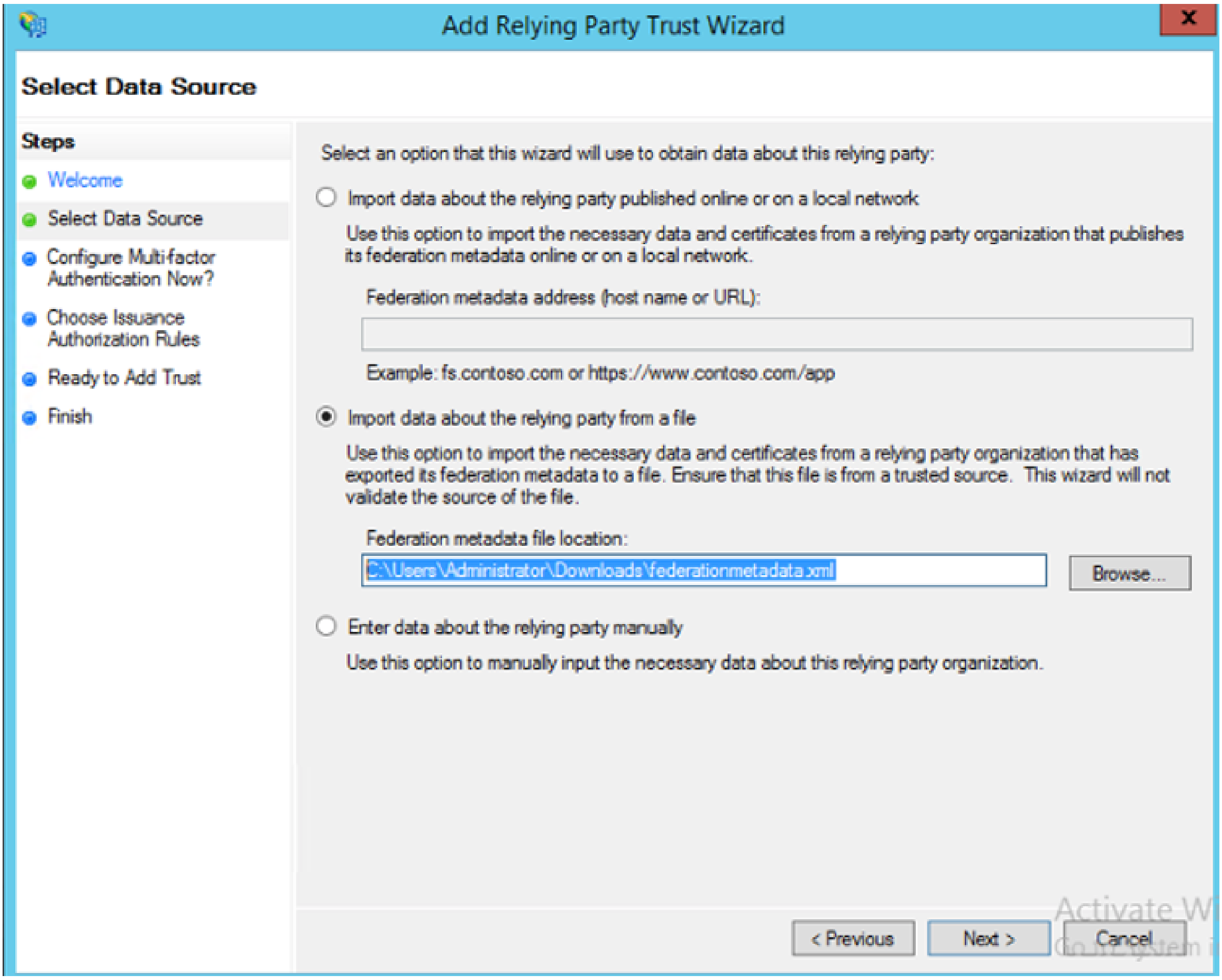
Welcome to the Add Relying Party Trust Wizard

This wizard will help you add a new relying party trust to the AD FS configuration database. Relying parties consume claims in security tokens that are issued by this Federation Service to make authentication and authorization decisions.

The relying party trust that this wizard creates defines how this Federation Service recognizes the relying party and issues claims to it. You can define issuance transform rules for issuing claims to the relying party after you complete the wizard.

続行するには[開始]をクリックします。

以前に保存したfederationmedatada.xmlメタデータXMLファイルを選択し、「次へ」をクリックします。


Add Relying Party Trust Wizard
Steps
Welcome
Select Data Source
Configure Multi-factor Authentication Now?
Choose Issuance Authorization Rules
Ready to Add Trust
Finish
Browse...
< Previous
Next >
Cancel

Select Data Source

Select an option that this wizard will use to obtain data about this relying party:

○ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

● Import data about the relying party from a file

Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

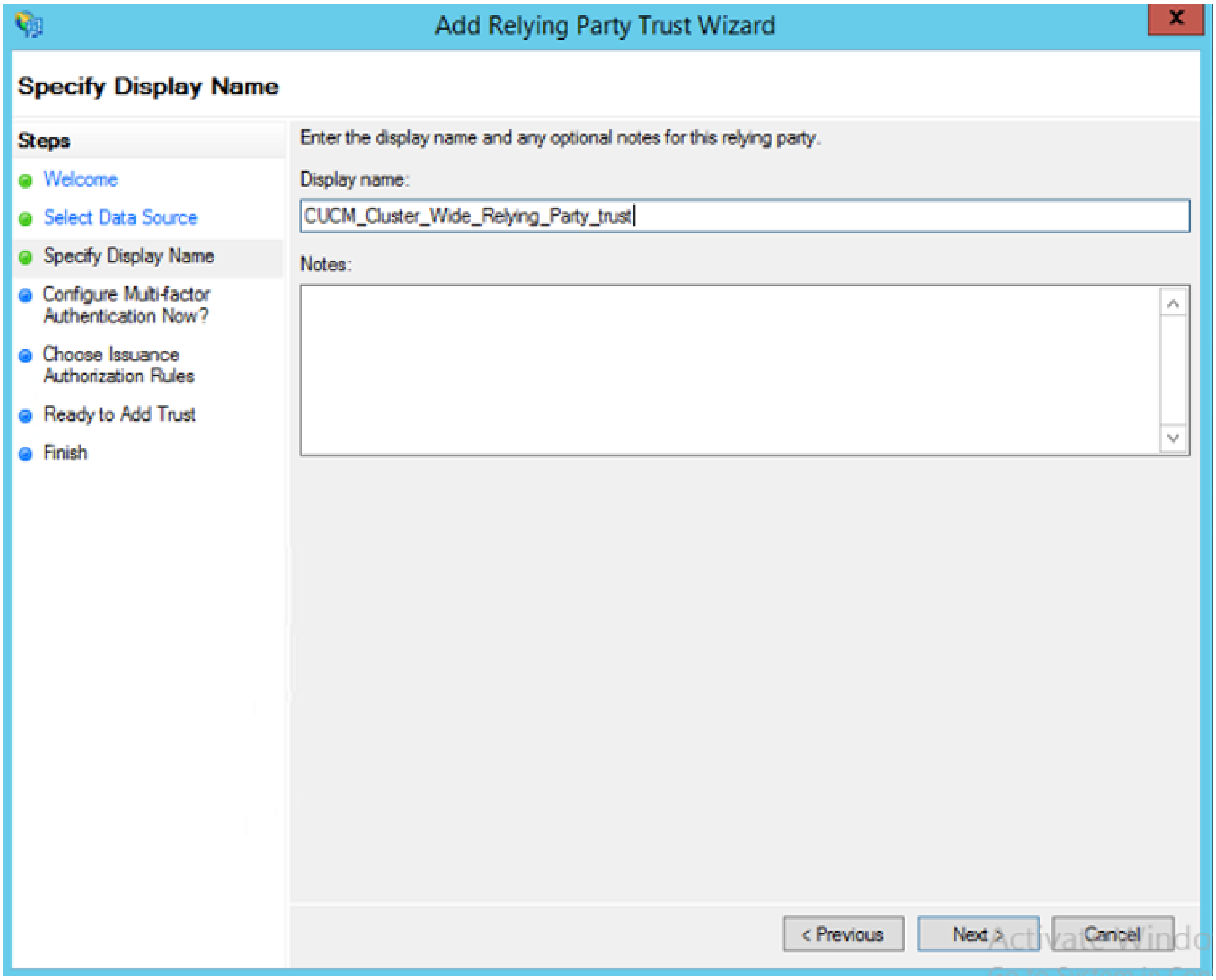
Federation metadata file location:

C:\Users\Administrator\Downloads\federationmetadata.xml

○ Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.

表示名としてCUCM_Cluster_Wide_Relying_Party_trustを使用し、[Next]をクリックします。



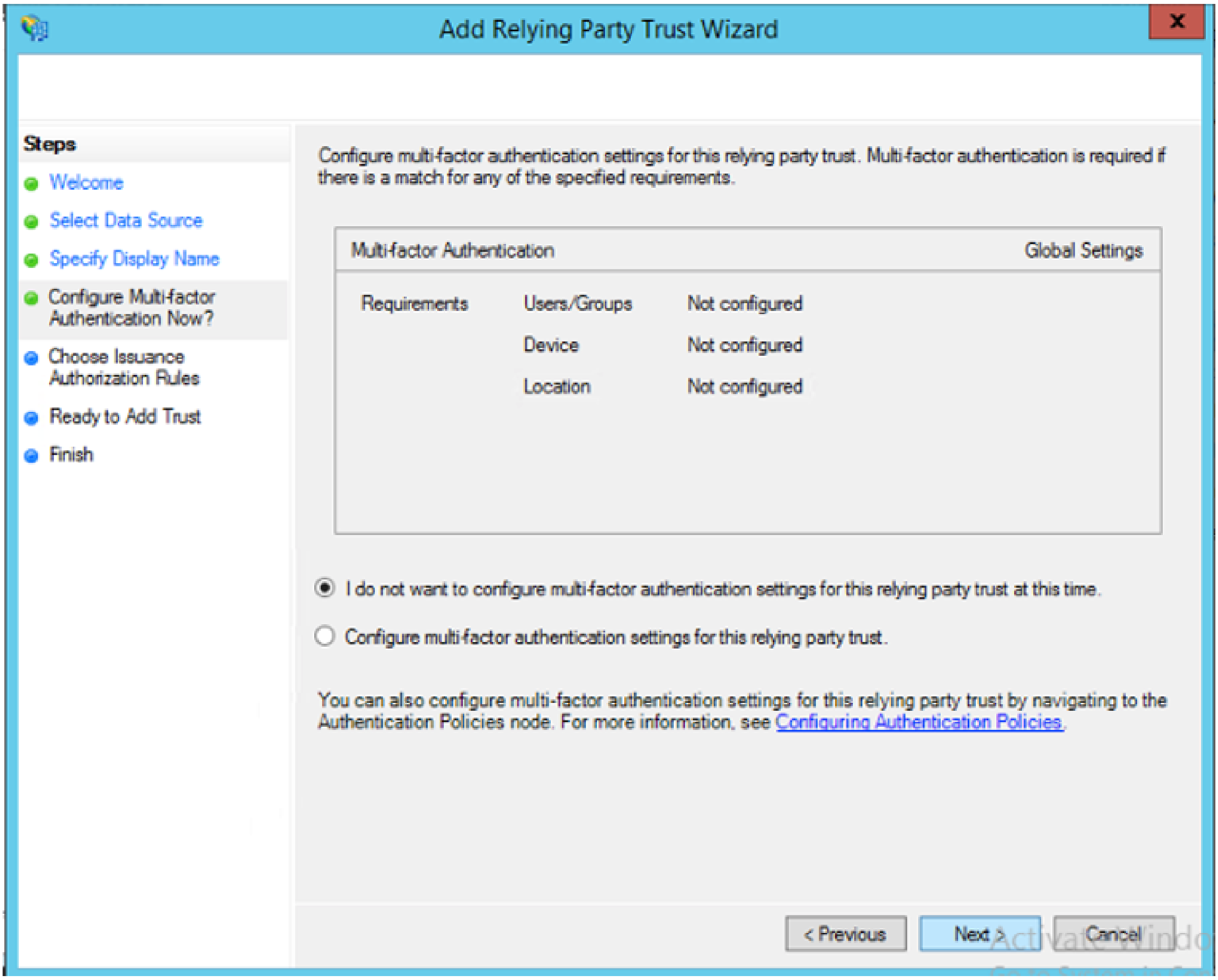
Enter the display name and any optional notes for this relying party.

Display name:

CUCM_Cluster_Wide_Relying_Party_trust

Notes:

最初のオプションを選択し、「次へ」をクリックします。



Add Relying Party Trust Wizard
Steps
Welcome
Select Data Source
Specify Display Name
Configure Multi-factor Authentication Now?
Choose Issuance Authorization Rules
Ready to Add Trust
Finish

Configure multi-factor authentication settings for this relying party trust. Multi-factor authentication is required if there is a match for any of the specified requirements.

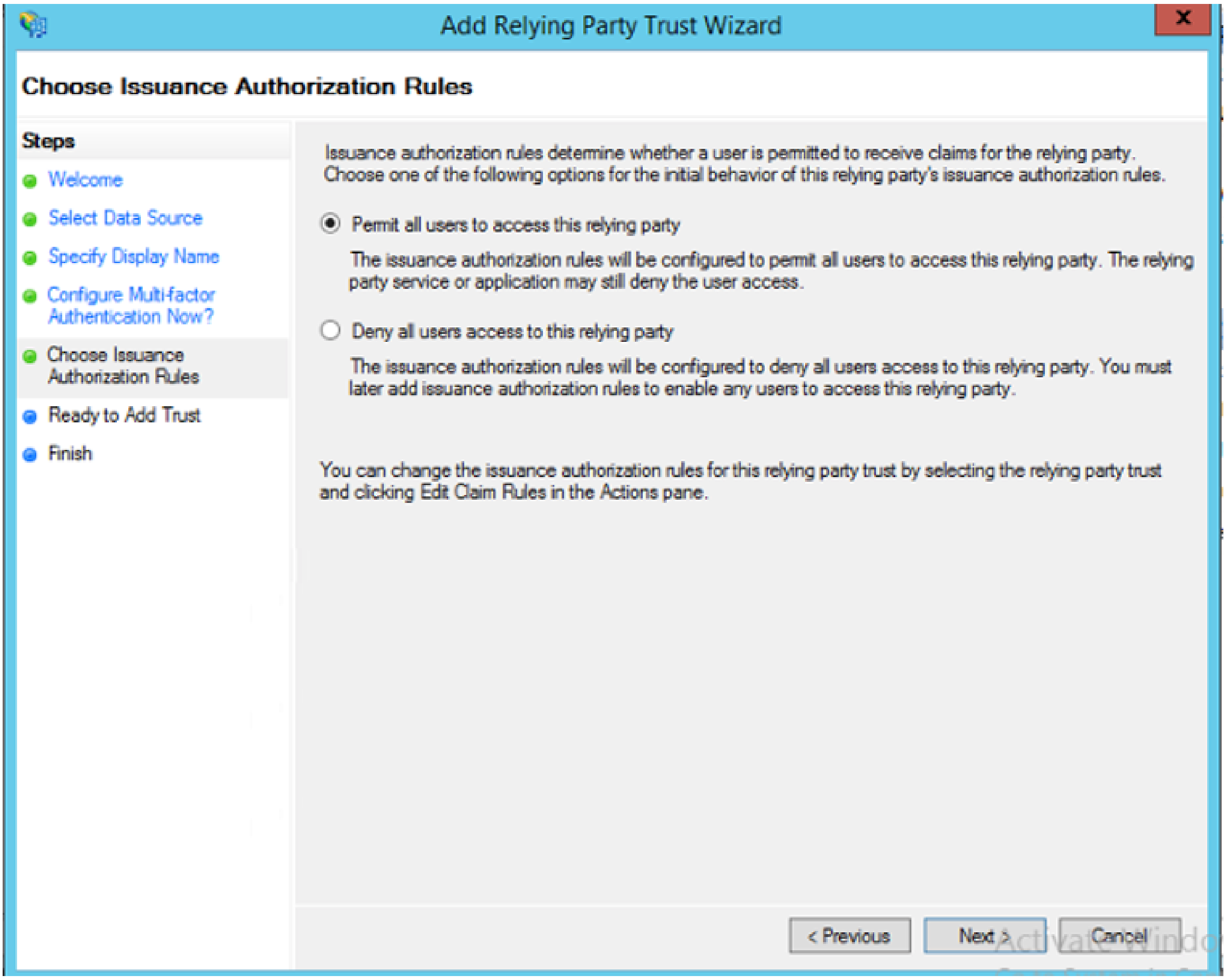
Multi-factor Authentication		Global Settings
Requirements	Users/Groups	Not configured
	Device	Not configured
	Location	Not configured

● I do not want to configure multi-factor authentication settings for this relying party trust at this time.

○ Configure multi-factor authentication settings for this relying party trust.

You can also configure multi-factor authentication settings for this relying party trust by navigating to the Authentication Policies node. For more information, see Configuring Authentication Policies.

[Permit all users to **access this relying party]を選択し、図に示すように[Next]**をクリックします。



Add Relying Party Trust Wizard

Choose Issuance Authorization Rules

Steps
Welcome
Select Data Source
Specify Display Name
Configure Multi-factor Authentication Now?
Choose Issuance Authorization Rules
Ready to Add Trust
Finish

Issuance authorization rules determine whether a user is permitted to receive claims for the relying party. Choose one of the following options for the initial behavior of this relying party's issuance authorization rules.

● Permit all users to access this relying party

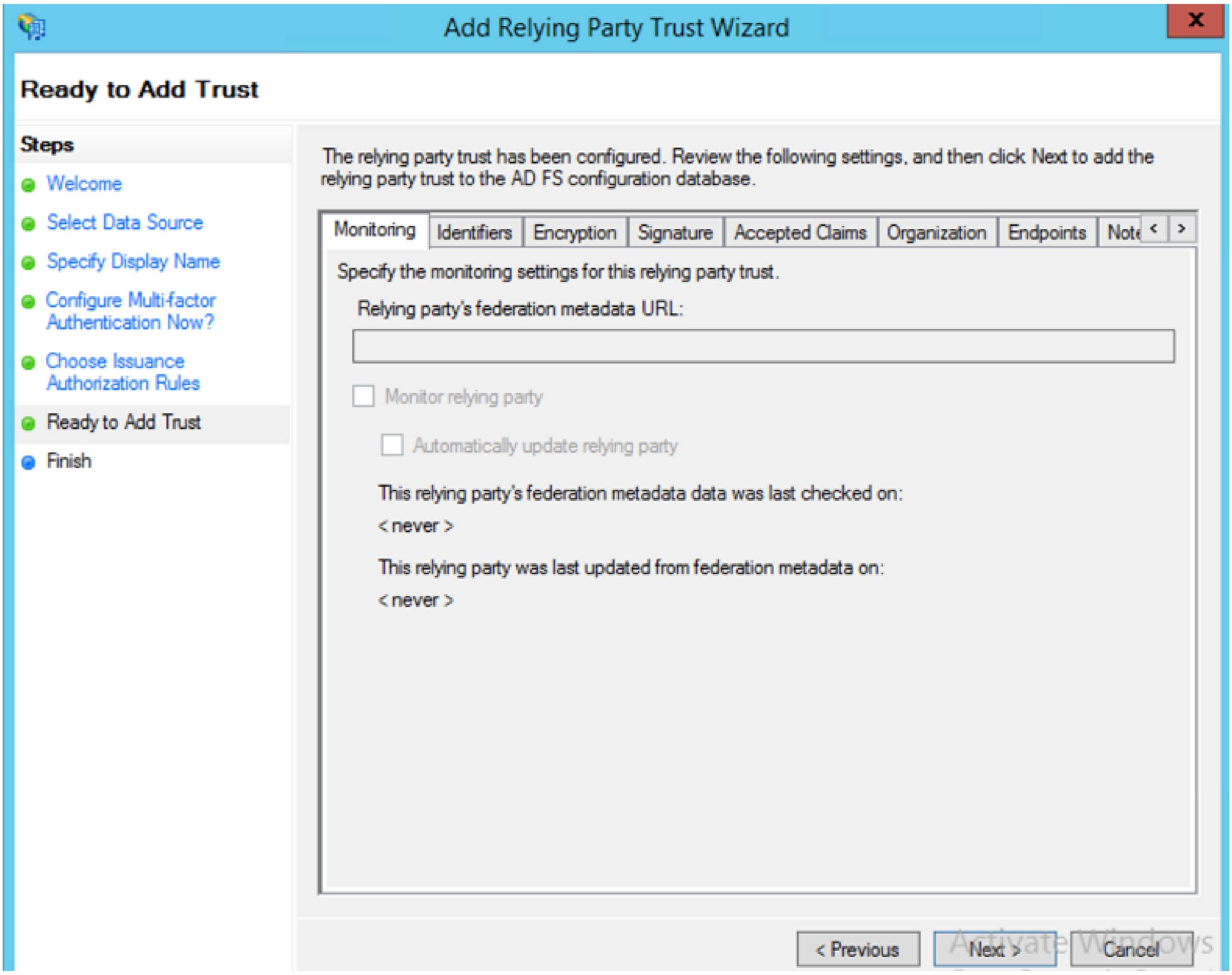
The issuance authorization rules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access.

○ Deny all users access to this relying party

The issuance authorization rules will be configured to deny all users access to this relying party. You must later add issuance authorization rules to enable any users to access this relying party.

You can change the issuance authorization rules for this relying party trust by selecting the relying party trust and clicking Edit Claim Rules in the Actions pane.

設定を確認し、図に示すように[Next]をクリックします。



Ready to Add Trust

The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.

Specify the monitoring settings for this relying party trust.

Relying party's federation metadata URL:

□ Monitor relying party

□ Automatically update relying party

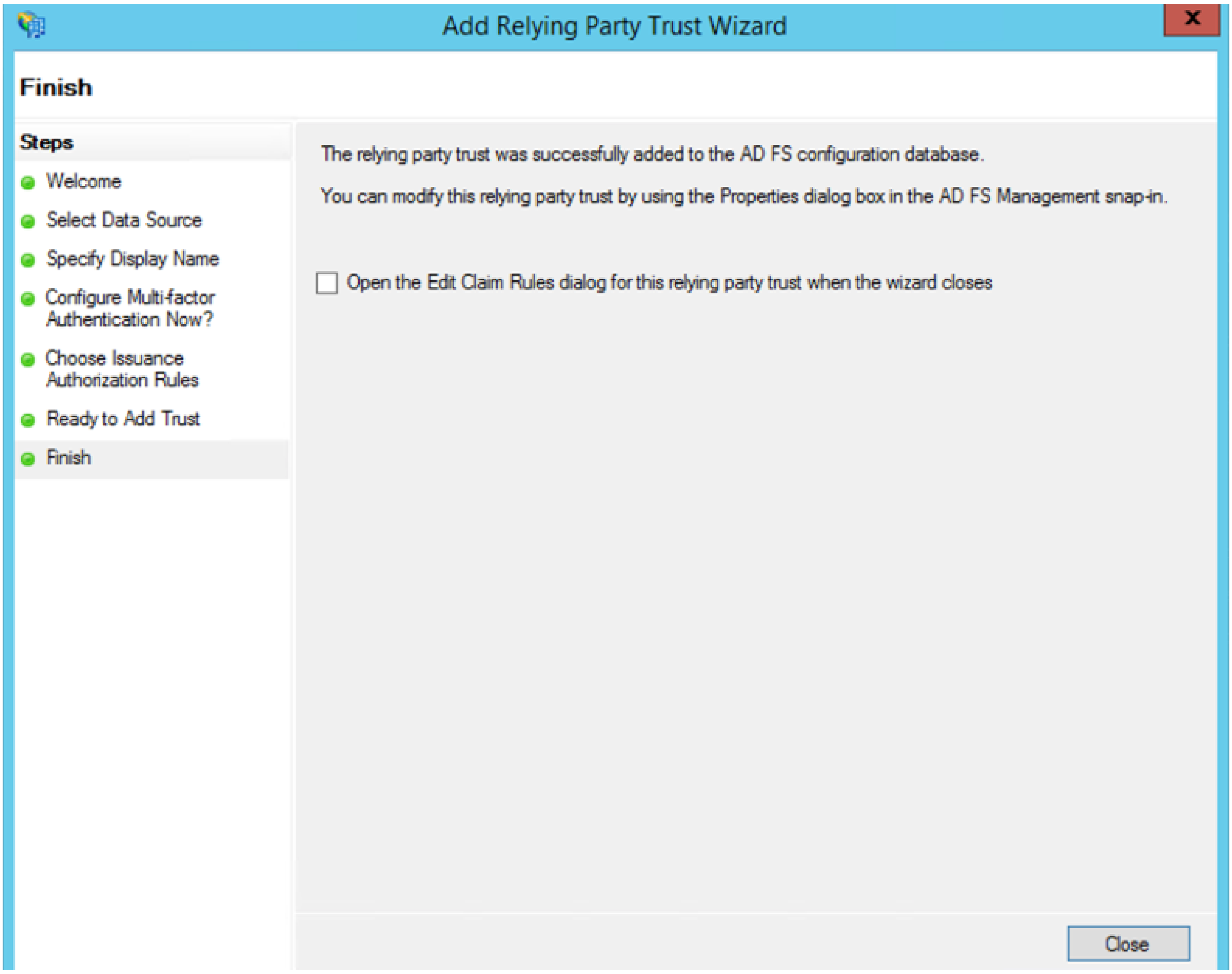
This relying party's federation metadata data was last checked on:

< never >

This relying party was last updated from federation metadata on:

< never >

チェックボックスをオフにして、[閉じる]をクリックします。

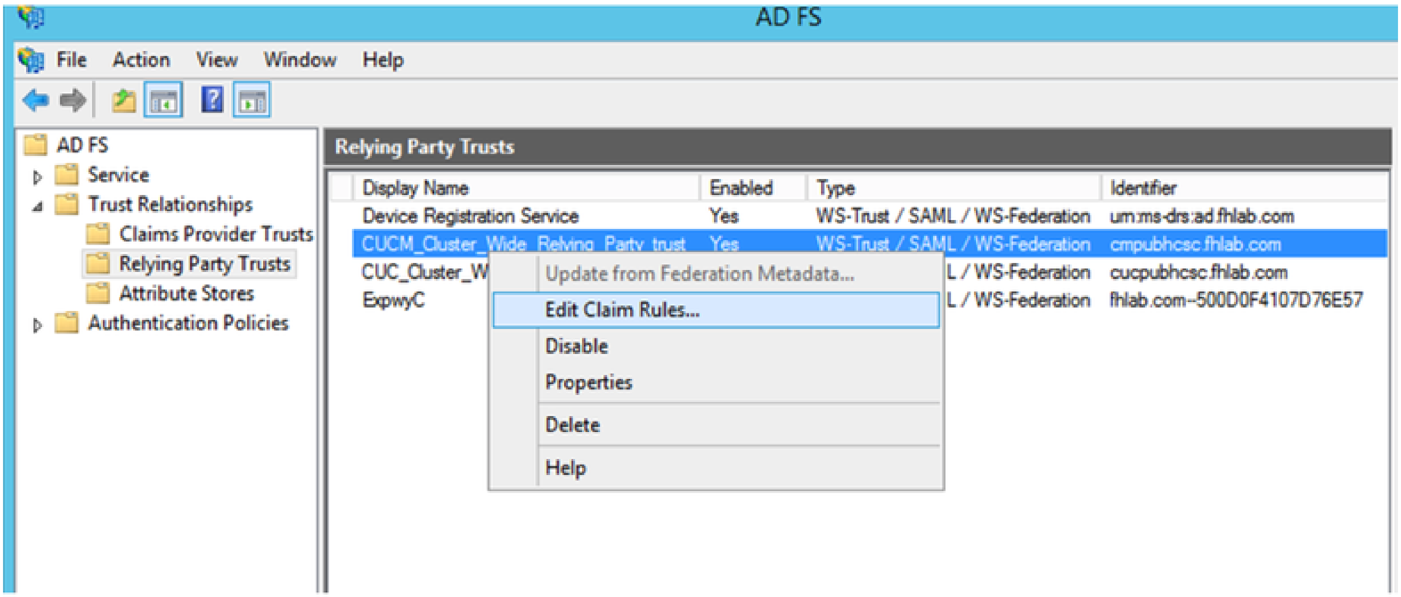

Add Relying Party Trust Wizard
Finish
Steps
Welcome
Select Data Source
Specify Display Name
Configure Multi-factor Authentication Now?
Choose Issuance Authorization Rules
Ready to Add Trust
Finish
Close

The relying party trust was successfully added to the AD FS configuration database.

You can modify this relying party trust by using the Properties dialog box in the AD FS Management snap-in.

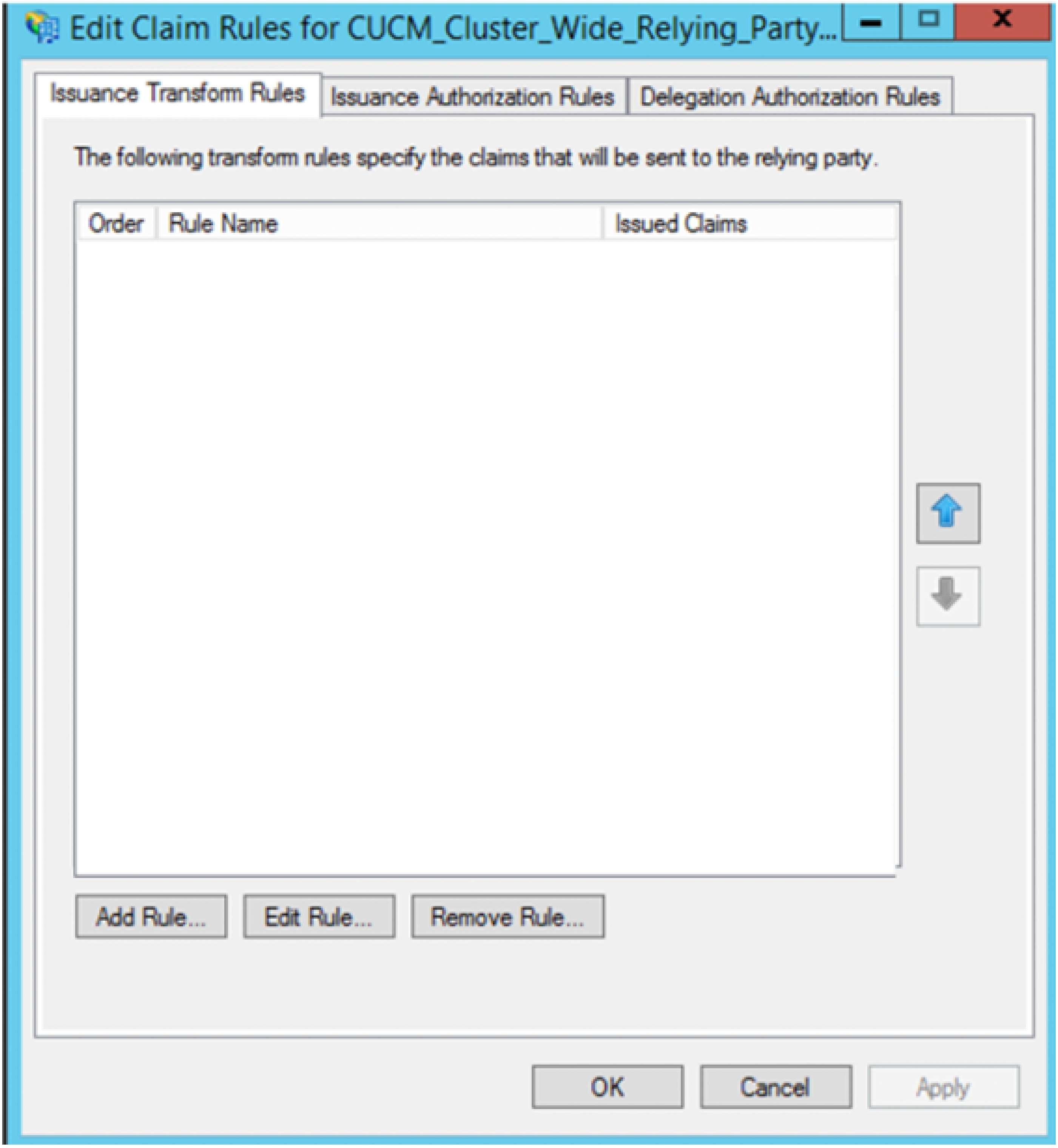
□ Open the Edit Claim Rules dialog for this relying party trust when the wizard closes

図に示すように、マウスの二次ボタンを使用し**て、作成し**た証明書利用者の信頼を選択し、**要求ルール**の構成を編集します。



Display Name	Enabled	Type	Identifier
Device Registration Service	Yes	WS-Trust / SAML / WS-Federation	um:ms-drs:ad.fhlab.com
CUCM_Cluster_Wide_Relying_Party_trust	Yes	WS-Trust / SAML / WS-Federation	cmpubhcsc.fhlab.com
CUC_Cluster_W		L / WS-Federation	cucpubhcsc.fhlab.com
ExpwyC		L / WS-Federation	fhlab.com-500D0F4107D76E57

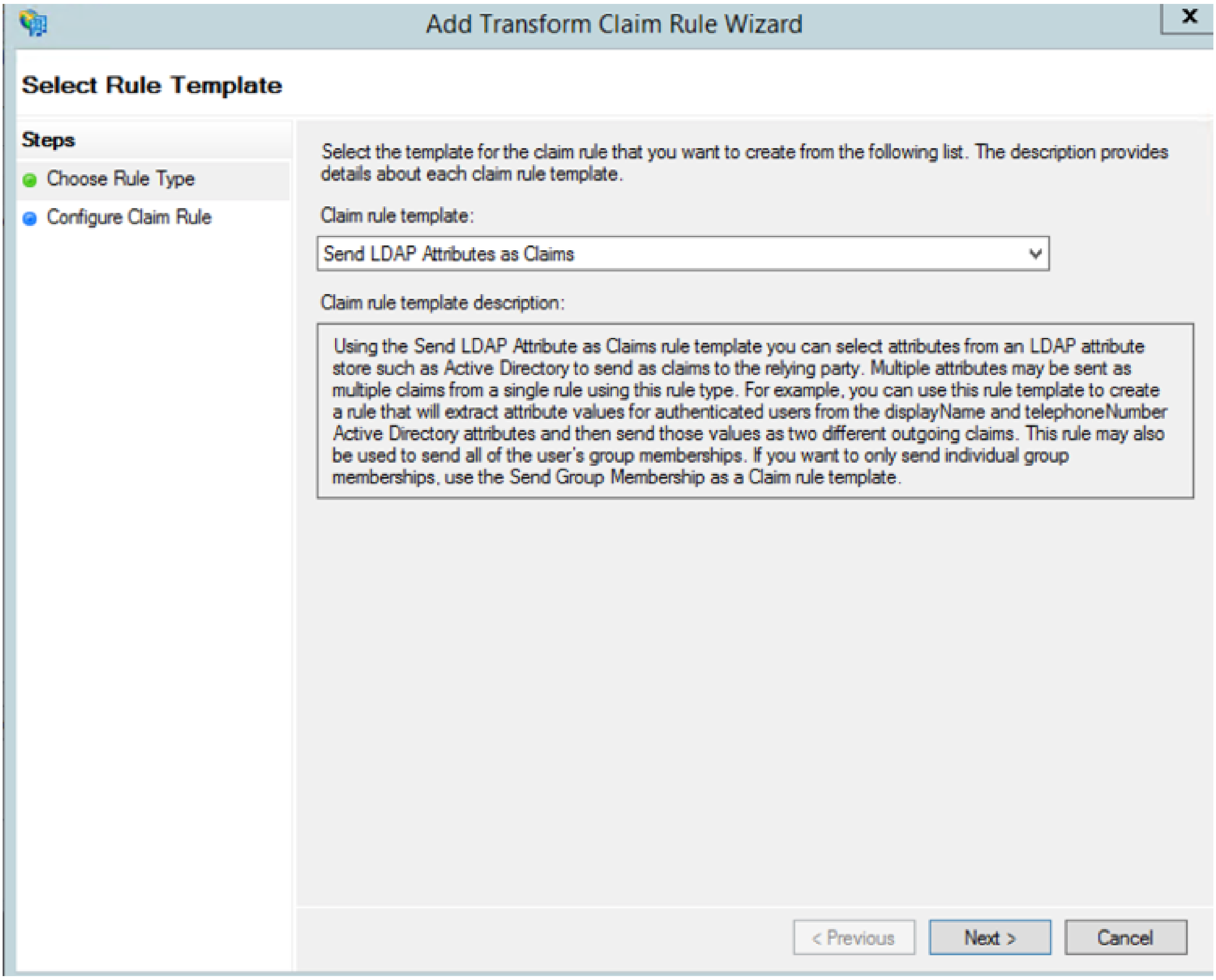
図に示すように[Add Rule]をクリックします。


Edit Claim Rules for CUCM_Cluster_Wide_Relying_Party...
Issuance Transform Rules
Issuance Authorization Rules
Delegation Authorization Rules
Add Rule...
Edit Rule...
Remove Rule...
OK
Cancel
Apply

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims

[Send LDAP Attributes as **Claims]を選択し、[Next]**をクリックします。



Add Transform Claim Rule Wizard

Select Rule Template

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template: Send LDAP Attributes as Claims

Claim rule template description:

Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.

次のパラメータを設定します。

クレームルール名：NameID

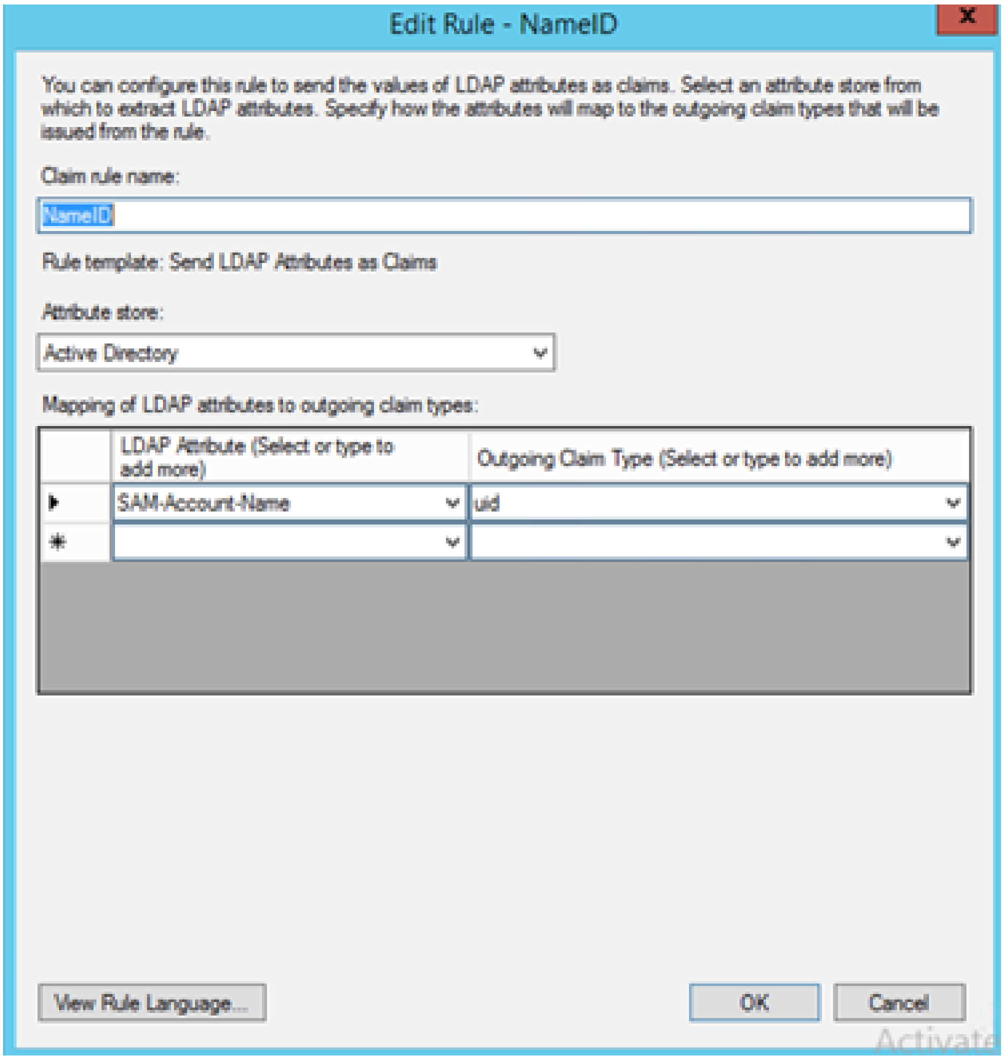
属性ストア：Active Directory（ドロップダウンメニューの矢印をダブルクリック）

LDAP 属性:SAM-Account-Name

送信要求の種類：uid

[FINISH/OK]をクリックして続行します。

uidは小文字ではなく、ドロップダウンメニューに存在しないことに注意してください。入力します。



Edit Rule - NameID

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

NameID

Rule template: Send LDAP Attributes as Claims

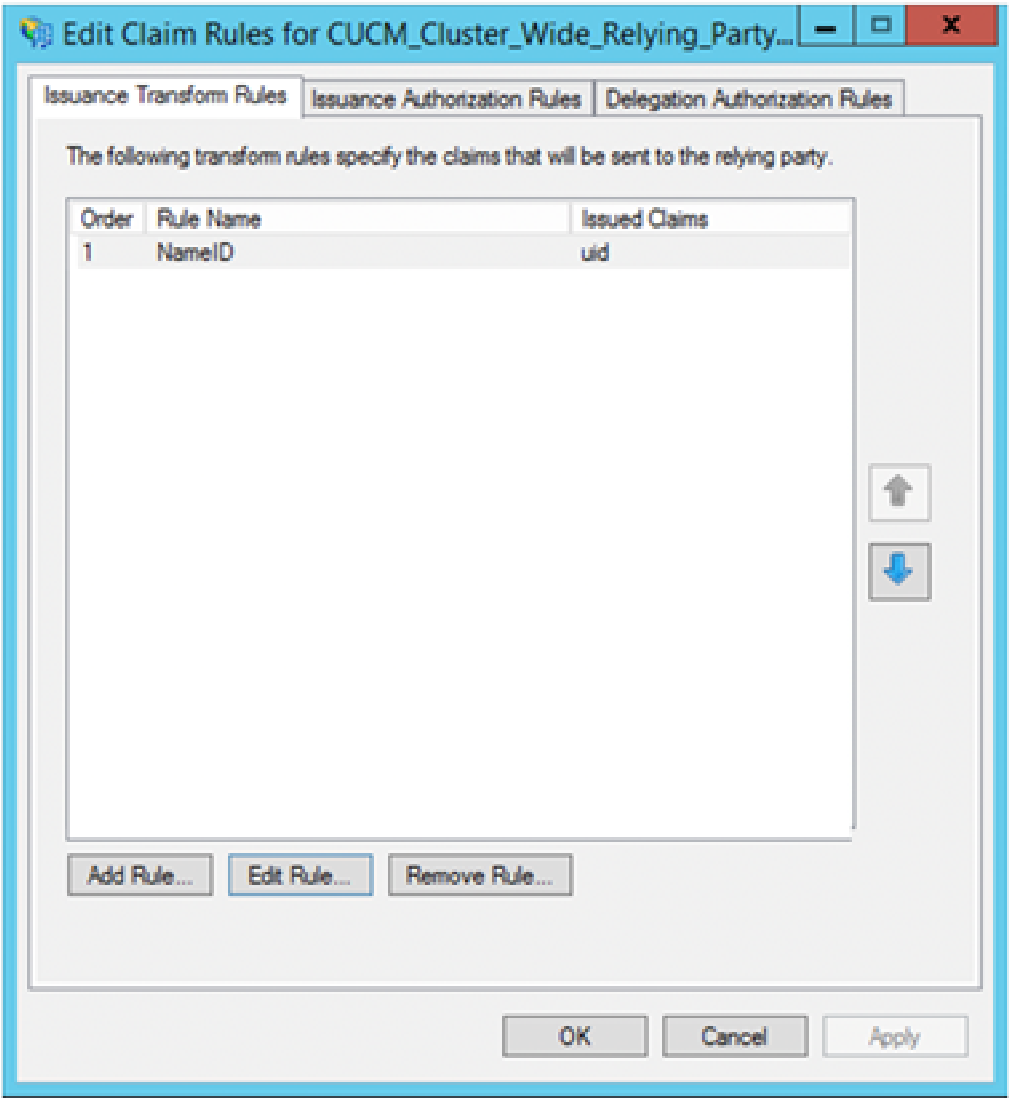
Attribute store:

Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	SAM-Account-Name	uid
*		

別のルールを追加するには、再度[Add Rule]をクリックします。

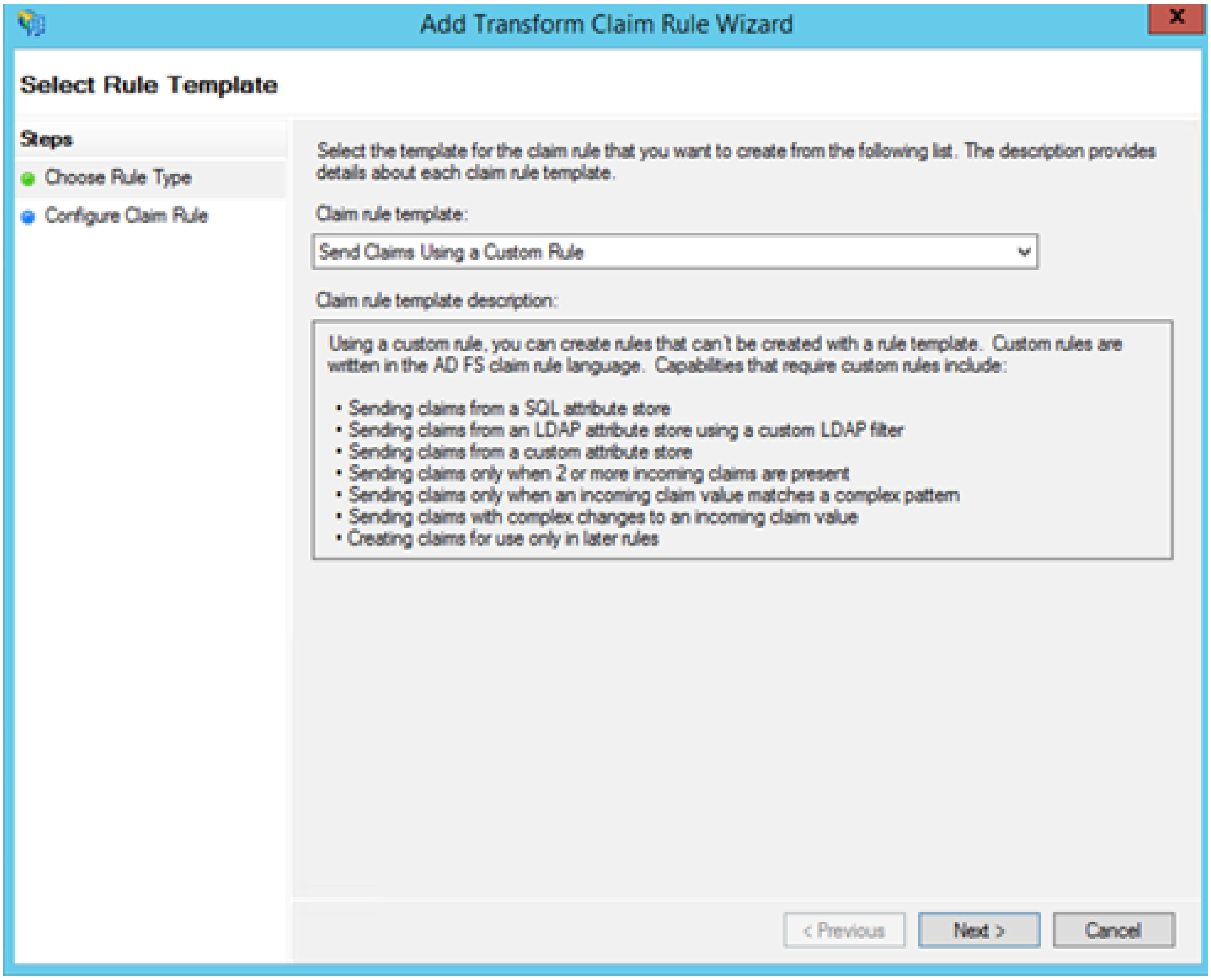

Edit Claim Rules for CUCM_Cluster_Wide_Relying_Party...
Issuance Transform Rules
Issuance Authorization Rules
Delegation Authorization Rules

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims
1	NameID	uid

Add Rule...
Edit Rule...
Remove Rule...
OK
Cancel
Apply

[Send Claims Using a **Custom Rule]を選択し、[Next**]をクリック**します。**



Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template:

Send Claims Using a Custom Rule

Claim rule template description:

Using a custom rule, you can create rules that can't be created with a rule template. Custom rules are written in the AD FS claim rule language. Capabilities that require custom rules include:

- Sending claims from a SQL attribute store
- Sending claims from an LDAP attribute store using a custom LDAP filter
- Sending claims from a custom attribute store
- Sending claims only when 2 or more incoming claims are present
- Sending claims only when an incoming claim value matches a complex pattern
- Sending claims with complex changes to an incoming claim value
- Creating claims for use only in later rules

Cluster_Side_Claim_Ruleというカスタムルールを作成します。

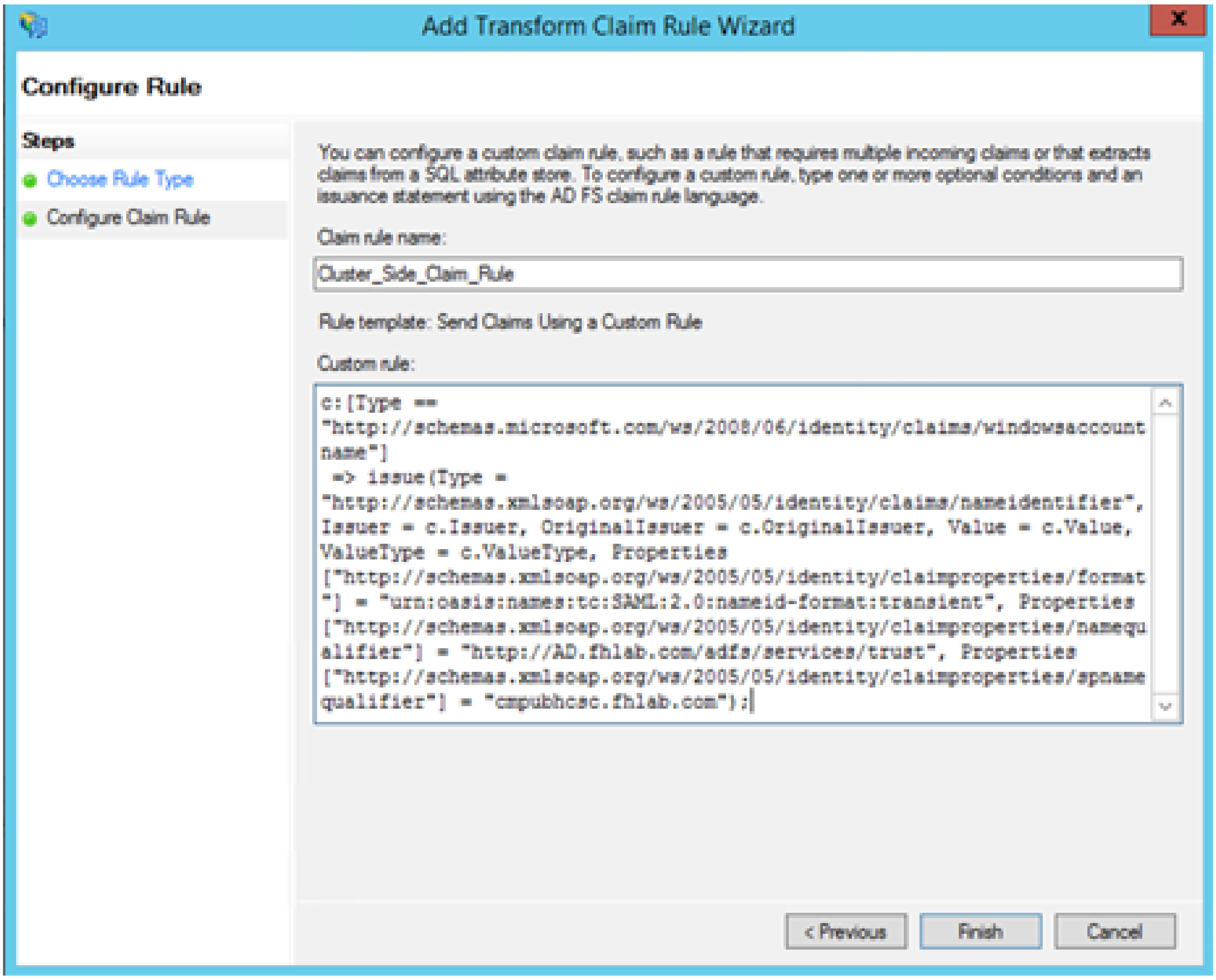
このテキストを、ここから直接ルールウィンドウにコピーアンドペーストします。テキストエディタで編集すると引用符が変更され、SSOをテストするときにルールが失敗する場合があります
。

```
c:[Type ==

"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]
=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"urn:oasis:names:tc:SAML:2.0:nameid-format:transient",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"]
= "http://<ADFS FQDN>/adfs/com/adfs/services/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =
"<CUCM Pub FQDN>");

c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]
=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"urn:oasis:names:tc:SAML:2.0:nameid-format:transient",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"] =
"http://AD.fhlab.com/adfs/services/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =
"cmpubhcsc.fhlab.com");
```

[完了]をクリックして続行します。



Configure Rule

You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS claim rule language.

Claim rule name:

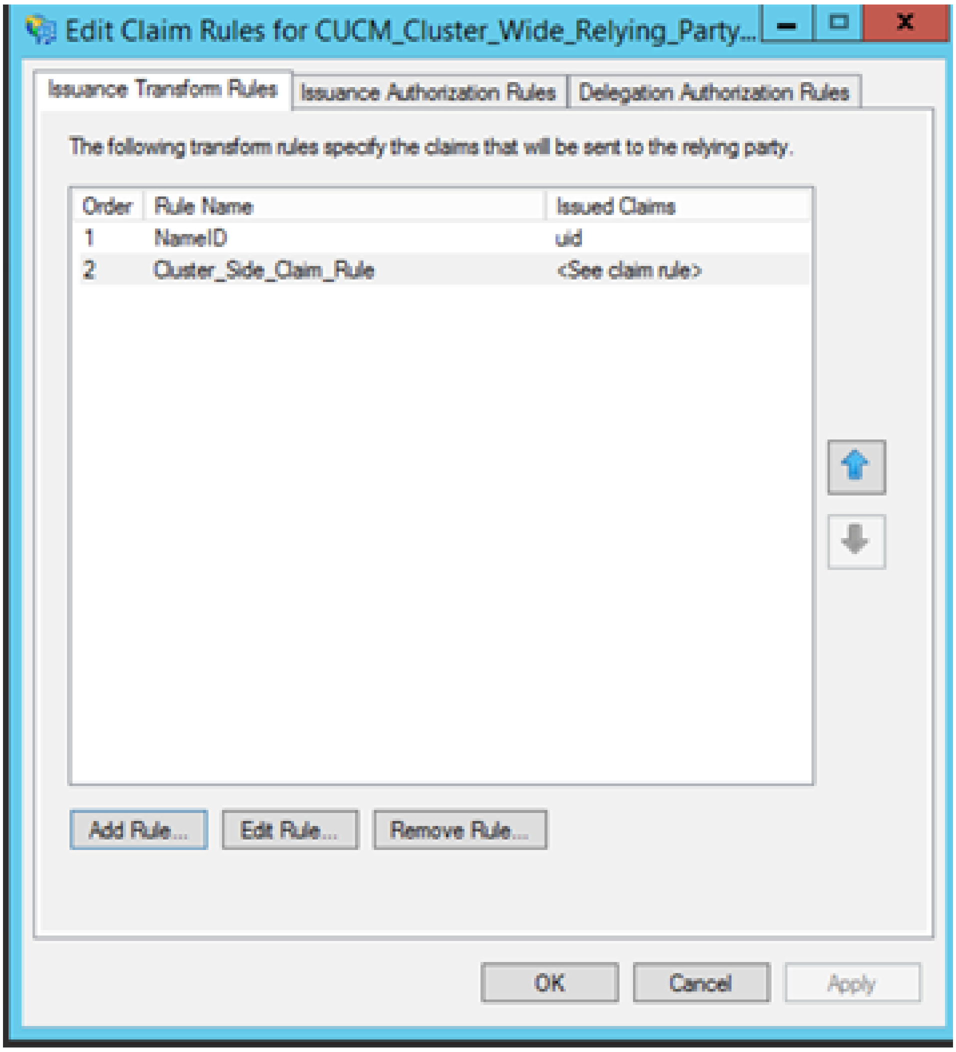
Cluster_Side_Claim_Rule

Rule template: Send Claims Using a Custom Rule

Custom rule:

```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccount
name"]
 => issue(Type =
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value,
ValueType = c.ValueType, Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format
"] = "urn:oasis:names:tc:SAML:2.0:nameid-format:transient", Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequ
alifier"] = "http://AD.fhlab.com/adfs/services/trust", Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spname
qualifier"] = "cmpubhcsc.fhlab.com");
```

これで、ADFSで2つのルールが定義されます。「適用」および「OK」をクリックし、ルール・ウィンドウを閉じます。

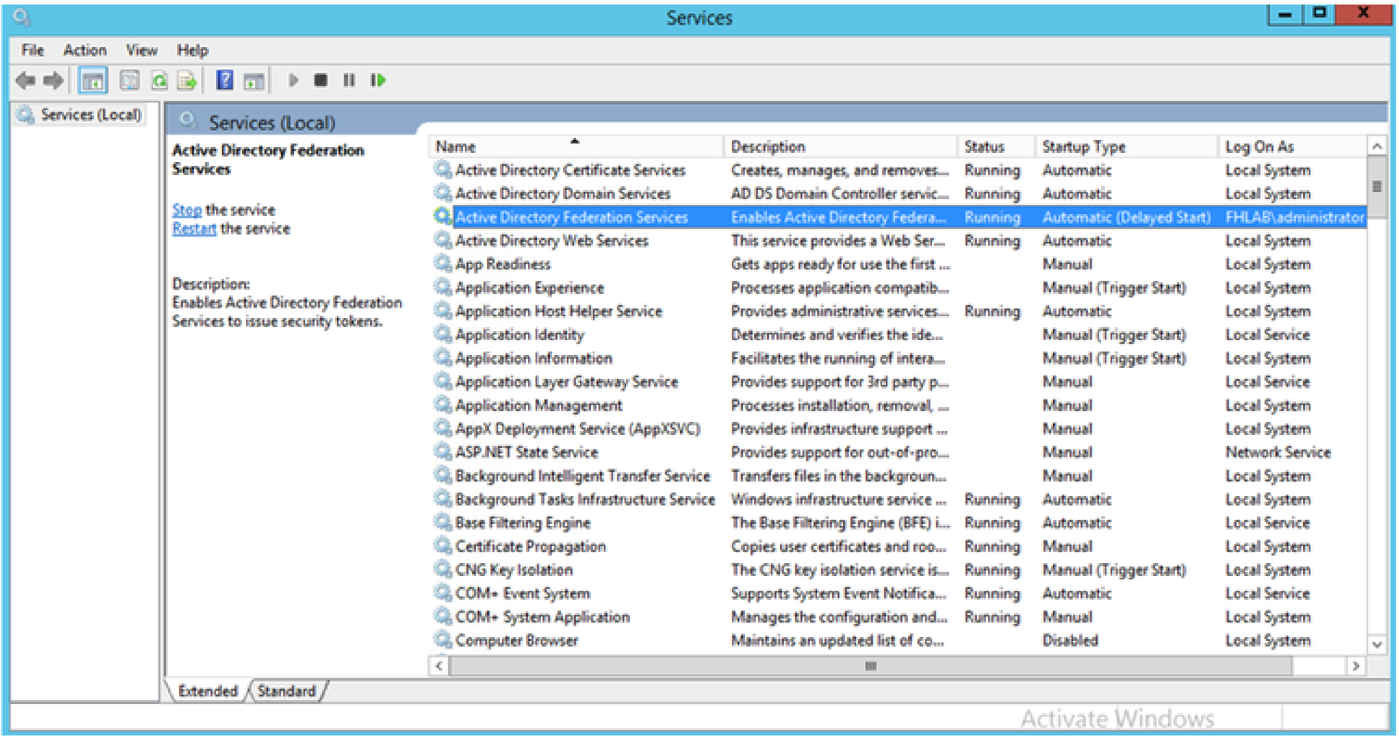


Edit Claim Rules for CUCM_Cluster_Wide_Relying_Party...
Issuance Transform Rules
Issuance Authorization Rules
Delegation Authorization Rules
Add Rule...
Edit Rule...
Remove Rule...
OK
Cancel
Apply

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims
1	NameID	uid
2	Cluster_Side_Claim_Rule	<See claim rule>

これで、CUCMが信頼できる証明書利用者としてADFSに正常に追加されました。



Active Directory Federation Services

Stop the service
Restart the service

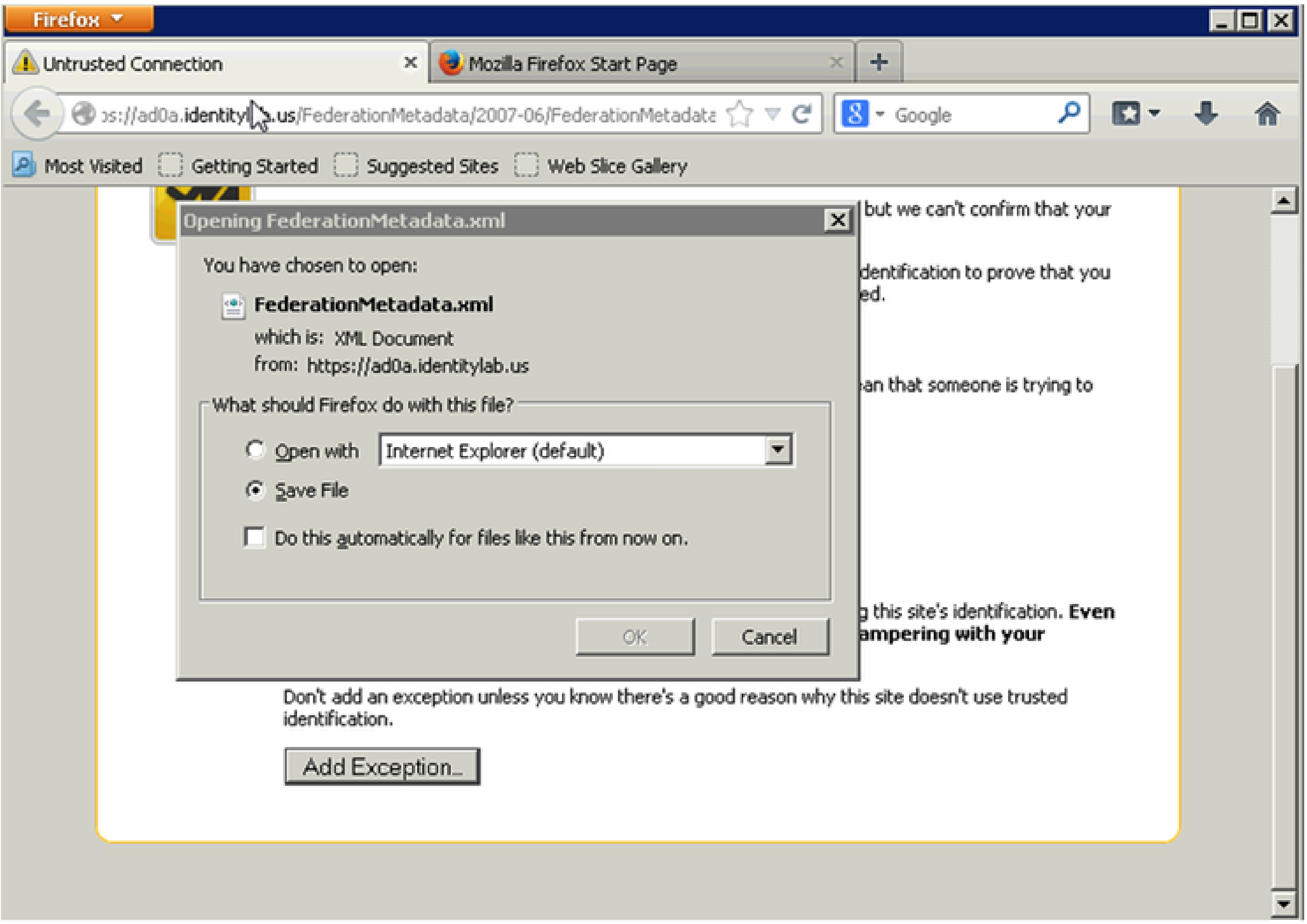
Description:
Enables Active Directory Federation Services to issue security tokens.

Name	Description	Status	Startup Type	Log On As
Active Directory Certificate Services	Creates, manages, and removes...	Running	Automatic	Local System
Active Directory Domain Services	AD DS Domain Controller servic...	Running	Automatic	Local System
Active Directory Federation Services	Enables Active Directory Federa...	Running	Automatic (Delayed Start)	FHLAB\administrator
Active Directory Web Services	This service provides a Web Ser...	Running	Automatic	Local System
App Readiness	Gets apps ready for use the first ...		Manual	Local System
Application Experience	Processes application compatib...		Manual (Trigger Start)	Local System
Application Host Helper Service	Provides administrative services...	Running	Automatic	Local System
Application Identity	Determines and verifies the ide...		Manual (Trigger Start)	Local Service
Application Information	Facilitates the running of intera...		Manual (Trigger Start)	Local System
Application Layer Gateway Service	Provides support for 3rd party p...		Manual	Local Service
Application Management	Processes installation, removal, ...		Manual	Local System
AppX Deployment Service (AppXSVC)	Provides infrastructure support ...		Manual	Local System
ASP.NET State Service	Provides support for out-of-pro...		Manual	Network Service
Background Intelligent Transfer Service	Transfers files in the backgroun...		Manual	Local System
Background Tasks Infrastructure Service	Windows infrastructure service ...	Running	Automatic	Local System
Base Filtering Engine	The Base Filtering Engine (BFE) i...	Running	Automatic	Local Service
Certificate Propagation	Copies user certificates and roo...	Running	Manual	Local System
CNG Key Isolation	The CNG key isolation service is...	Running	Manual (Trigger Start)	Local System
COM+ Event System	Supports System Event Notifica...	Running	Automatic	Local Service
COM+ System Application	Manages the configuration and...	Running	Manual	Local System
Computer Browser	Maintains an updated list of co...		Disabled	Local System

続行する前に、ADFSサービスを再起動してください。[スタート**メニュー] > [管理ツール] > [サービス]に移動します。**

IDPメタデータ

CUCMにIdPに関する情報を提供する必要があります。この情報は、XMLメタデータを使用して交換されます。ADFSがインストールされているサーバでこの手順を実行してください。



Opening FederationMetadata.xml

You have chosen to open:

FederationMetadata.xml

which is: XML Document

from: https://ad0a.identitylab.us

What should Firefox do with this file?

○ Open with Internet Explorer (default)

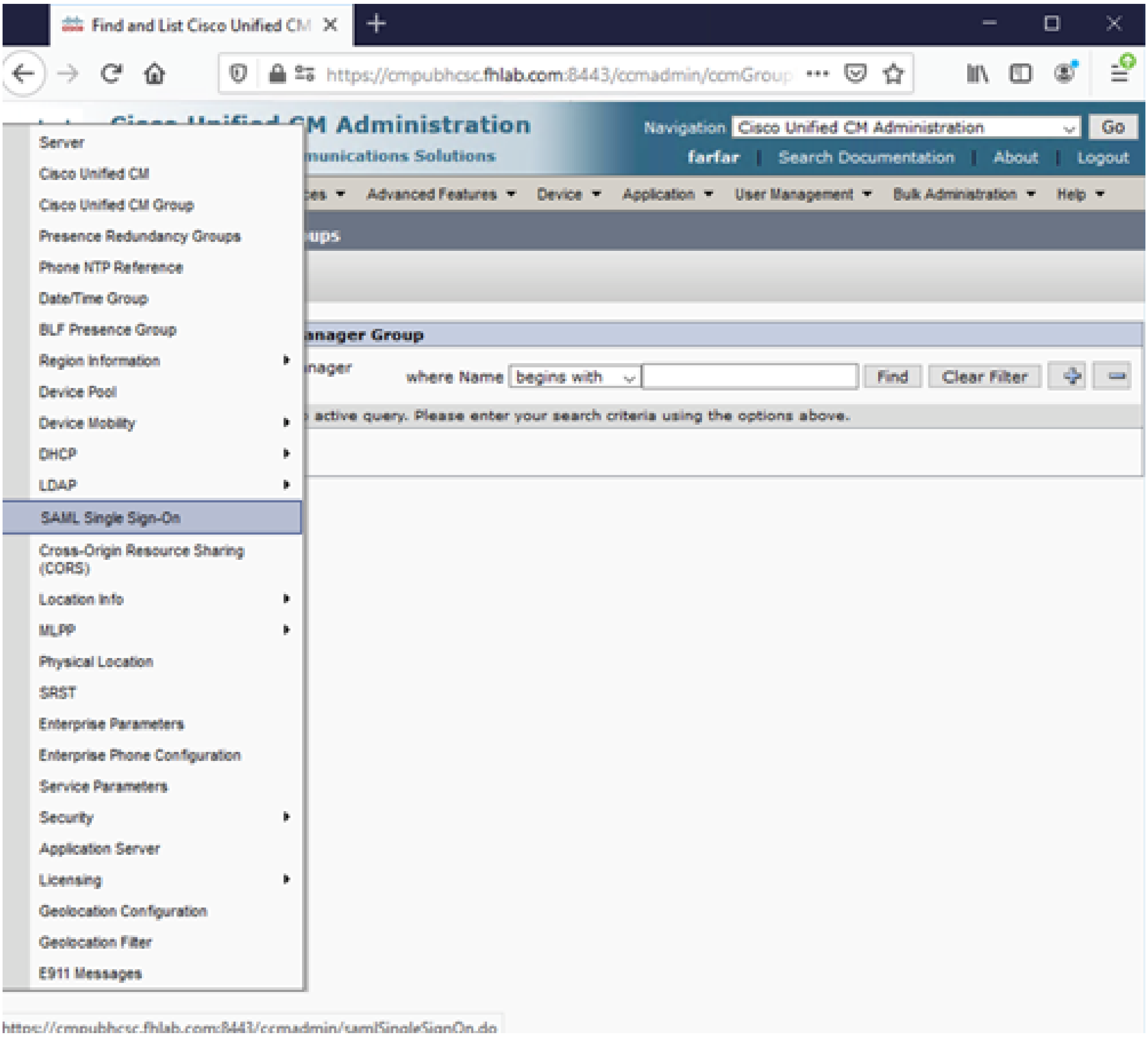
● Save File

□ Do this automatically for files like this from now on.

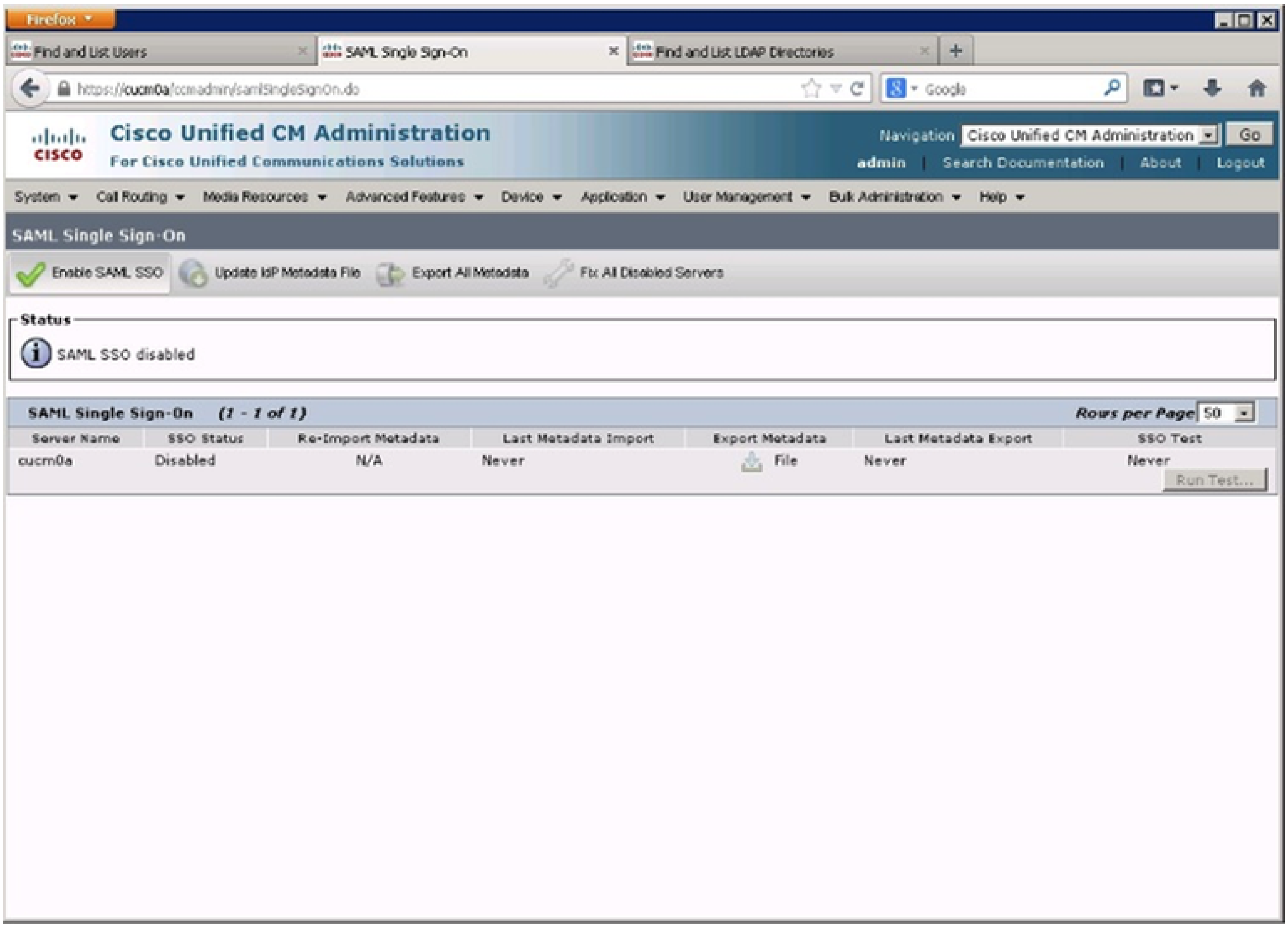
Firefox
Untrusted Connection
Mozilla Firefox Start Page
ps://ad0a.identity.us/FederationMetadata/2007-06/FederationMetadata
Google
Most Visited
Getting Started
Suggested Sites
Web Slice Gallery
OK
Cancel
but we can't confirm that your
dentification to prove that you
ed.
an that someone is trying to
g this site's identification. Even
ampering with your
Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.
Add Exception...

まず、Firefoxブラウザを使用してADFS(IdP)に接続し、XMLメタデータをダウンロードする必要があります。ブラウザでhttps://<ADFS FQDN>/FederationMetadata/2007-06/FederationMetadata.xmlを開き、メタデータをローカルフォルダに保存します。

ここで、[CUCM configuration]に移動し、**[System Menu] > [SAML Single Sign-On]メニューに移動します。**



CUCM Administrationに戻り、[SYSTEM] > [SAML Single Sign-On]を選択します。


Firefox
Find and List Users
SAML Single Sign-On
Find and List LDAP Directories
https://cucm0a/ccmadmin/samlSingleSignOn.do
Google
Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
admin | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help
Enable SAML SSO
Update IdP Metadata File
Export All Metadata
Fix All Disabled Servers
Run Test...

SAML Single Sign-On

Status

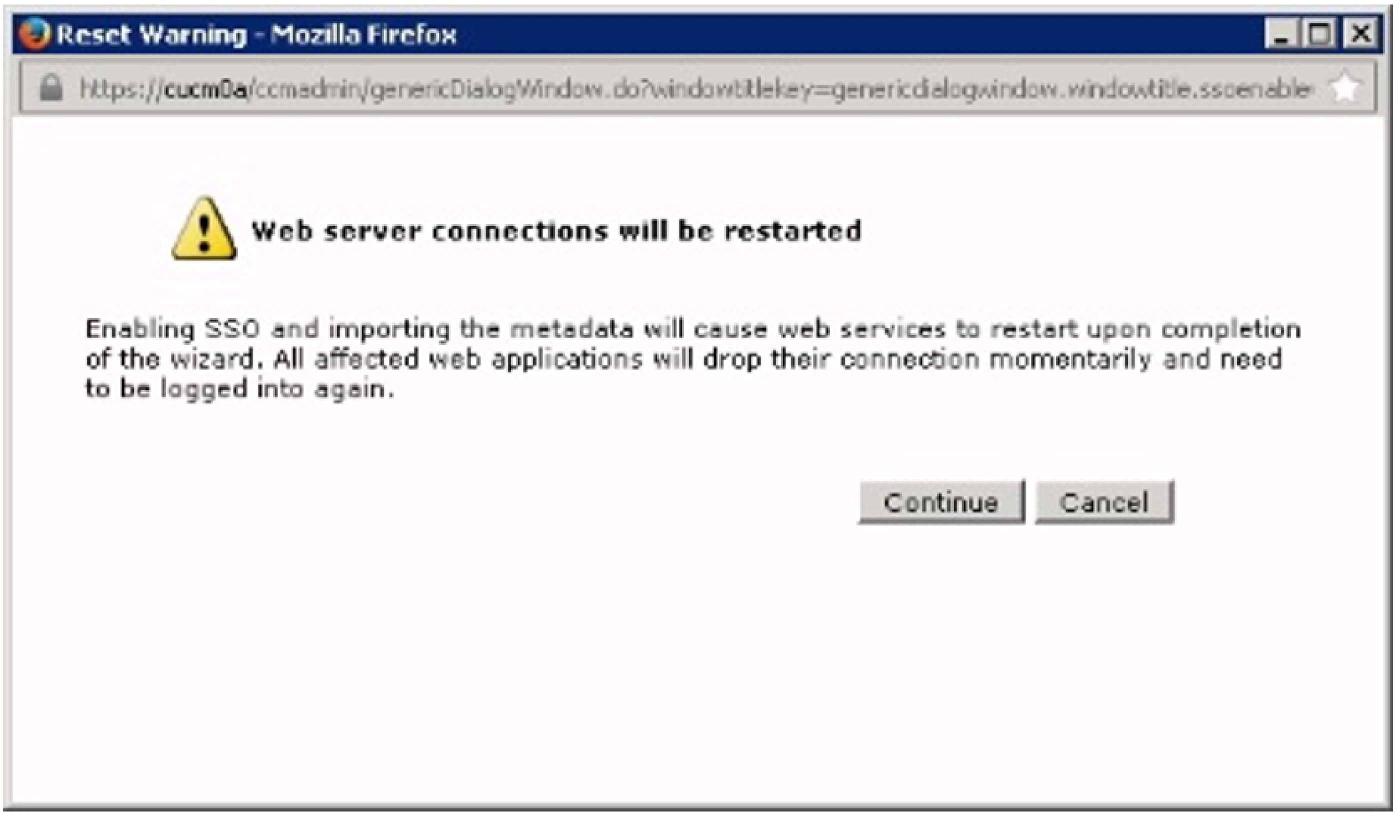
SAML SSO disabled

SAML Single Sign-On (1 - 1 of 1) Rows per Page 50

Server Name	SSO Status	Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	SSO Test
cucm0a	Disabled	N/A	Never	File	Never	Never

[Enable SAML SSO]を選択します。

[Continue]をクリックして、警告を確認します。

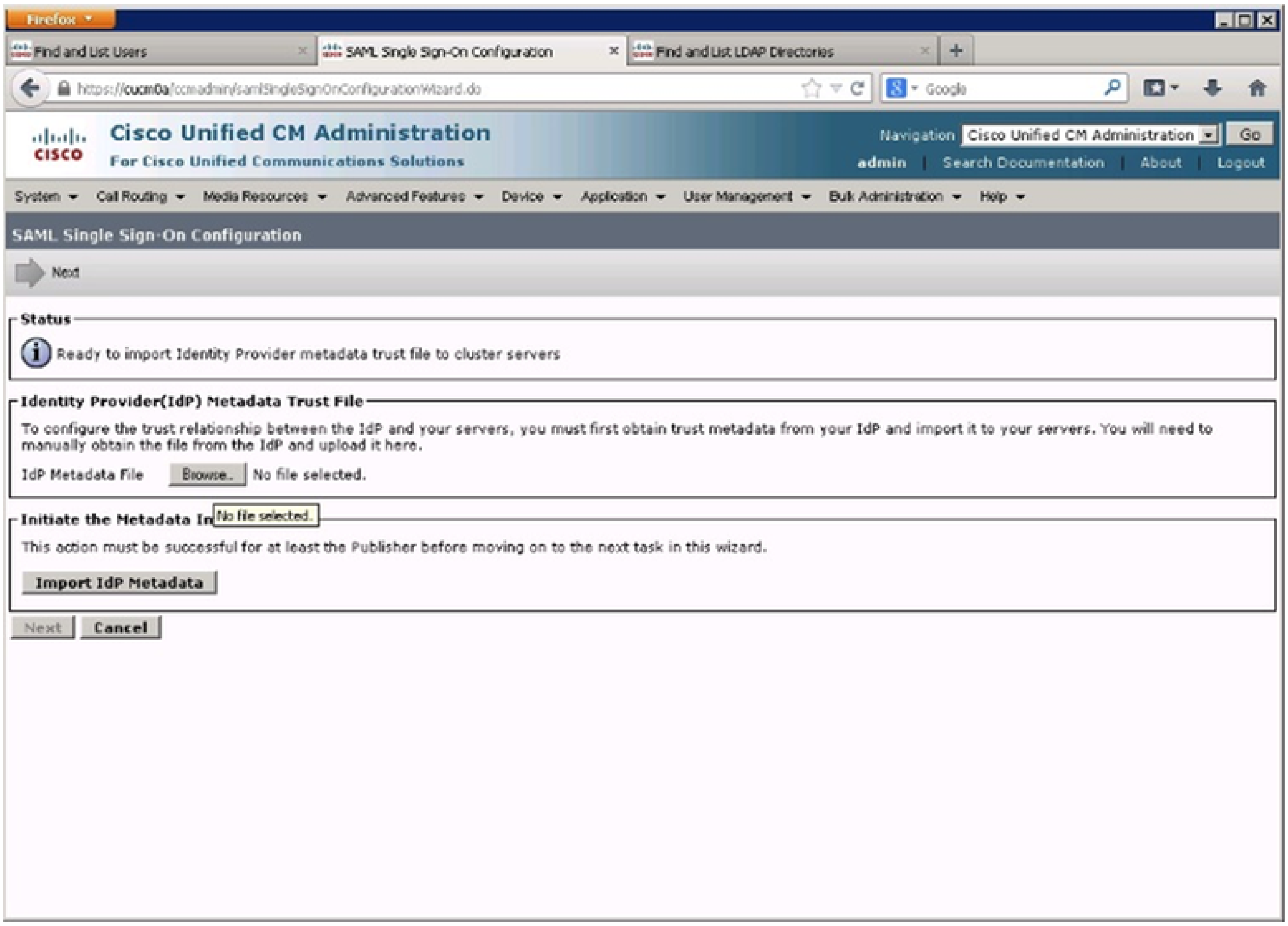

Reset Warning - Mozilla Firefox
https://cucm0a/ccmadmin/genericDialogWindow.do?windowtitlekey=genericdialogwindow.windowtitle.ssoenable
Continue
Cancel

Web server connections will be restarted

Enabling SSO and importing the metadata will cause web services to restart upon completion of the wizard. All affected web applications will drop their connection momentarily and need to be logged into again.

SSO画面で[Browse..]をクリックして、図に示すように、以前に保存した

FederationMetadata.xmlメタデータXMLファイルをインポートします。


Firefox
Find and List Users
SAML Single Sign-On Configuration
Find and List LDAP Directories
https://cucm0a/ccmadmin/samlSingleSignOnConfigurationWizard.do
Google
Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
admin | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help

SAML Single Sign-On Configuration

Next

Status

Ready to import Identity Provider metadata trust file to cluster servers

Identity Provider(IdP) Metadata Trust File

To configure the trust relationship between the IdP and your servers, you must first obtain trust metadata from your IdP and import it to your servers. You will need to manually obtain the file from the IdP and upload it here.

IdP Metadata File Browse... No file selected.

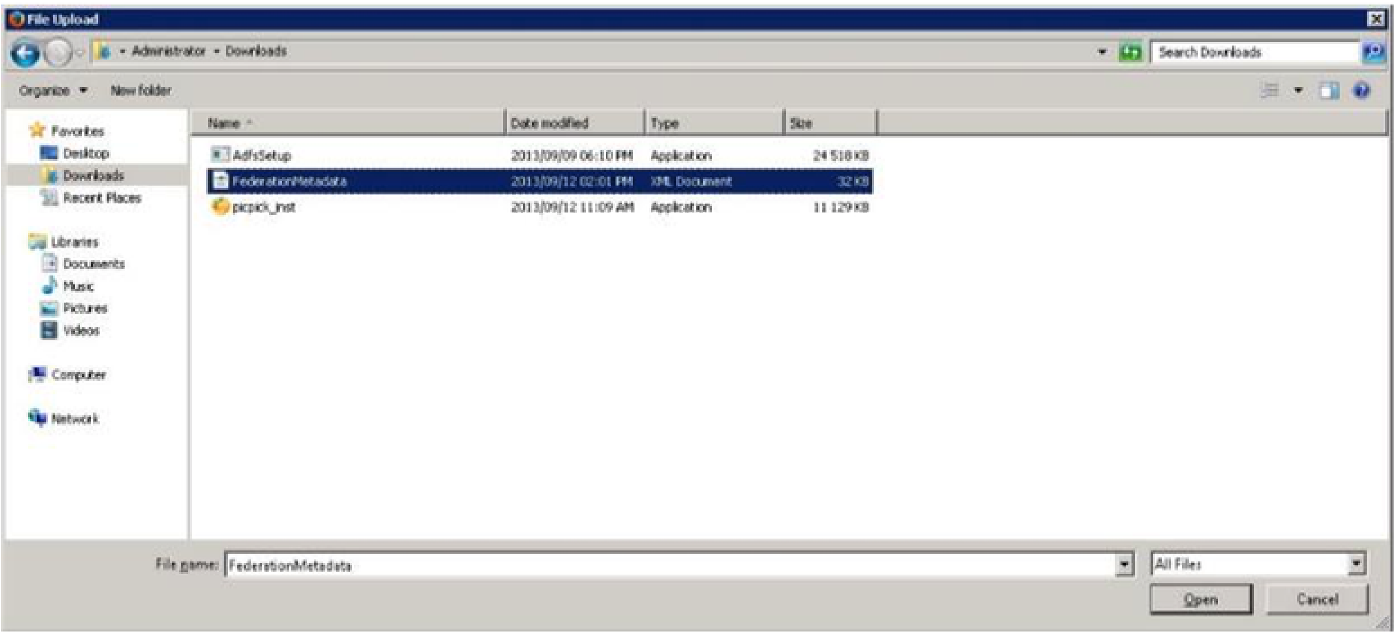
Initiate the Metadata In No file selected.

This action must be successful for at least the Publisher before moving on to the next task in this wizard.

Import IdP Metadata

Next Cancel

XMLファイルを選択し、[Open]をクリックして、[Downloads]の[Favorites]からCUCMにアップロードします。

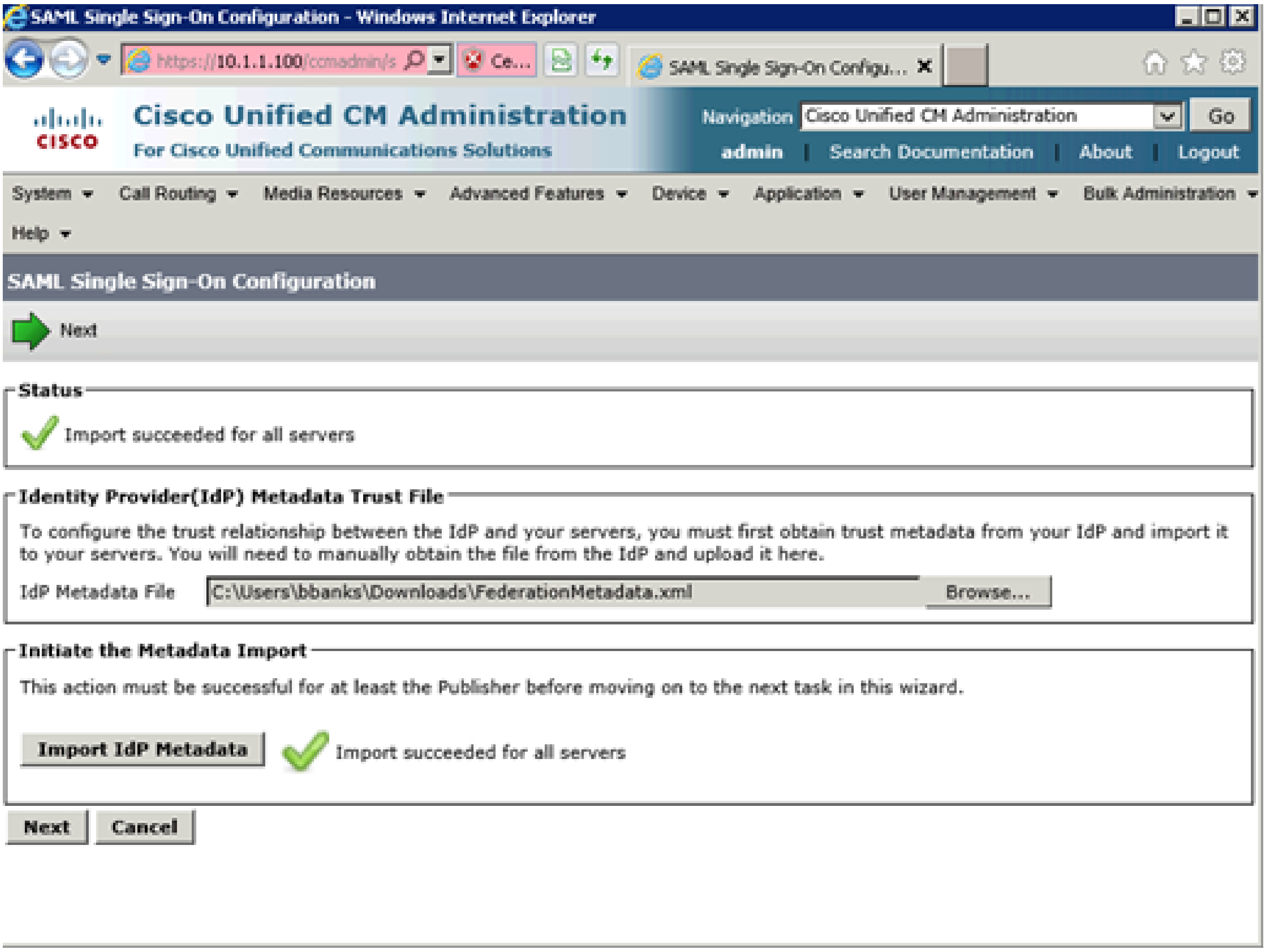


Name	Date modified	Type	Size
AdfsSetup	2013/09/09 06:10 PM	Application	24 518 KB
FederationMetadata	2013/09/12 02:01 PM	XML Document	32 KB
picpick_inst	2013/09/12 11:09 AM	Application	11 129 KB

File name: FederationMetadata All Files

Open Cancel

アップロードが完了したら、[Import IdP Metadata]をクリックして、IdP情報をCUCMにインポートします。インポートが成功したことを確認し、[Next]をクリックして続行します。


SAML Single Sign-On Configuration - Windows Internet Explorer
https://10.1.1.100/ccmadmin/s
SAML Single Sign-On Configu...
Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
admin | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help

SAML Single Sign-On Configuration

Next

Status

✓ Import succeeded for all servers

Identity Provider(IdP) Metadata Trust File

To configure the trust relationship between the IdP and your servers, you must first obtain trust metadata from your IdP and import it to your servers. You will need to manually obtain the file from the IdP and upload it here.

IdP Metadata File C:\Users\bbanks\Downloads\FederationMetadata.xml Browse...

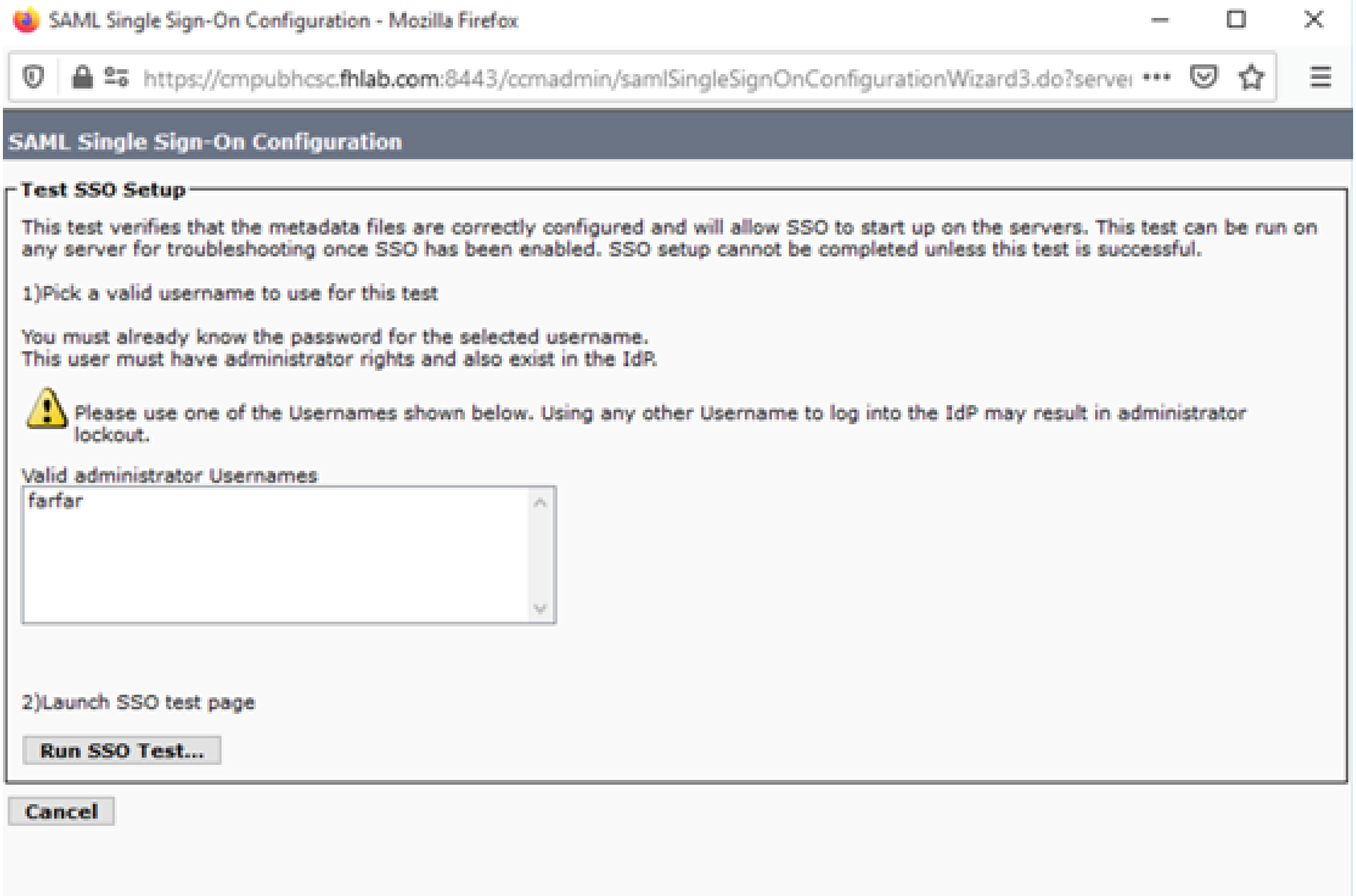
Initiate the Metadata Import

This action must be successful for at least the Publisher before moving on to the next task in this wizard.

Import IdP Metadata ✓ Import succeeded for all servers

Next Cancel

[Standard CCM Super Users]に属するユーザを選択し、[RUN SSO TEST]をクリックします。


SAML Single Sign-On Configuration - Mozilla Firefox
https://cmpubhcsc.fhlab.com:8443/ccmadmin/samlSingleSignOnConfigurationWizard3.do?server

SAML Single Sign-On Configuration

Test SSO Setup

This test verifies that the metadata files are correctly configured and will allow SSO to start up on the servers. This test can be run on any server for troubleshooting once SSO has been enabled. SSO setup cannot be completed unless this test is successful.

1)Pick a valid username to use for this test

You must already know the password for the selected username.
This user must have administrator rights and also exist in the IdP.

⚠ Please use one of the Usernames shown below. Using any other Username to log into the IdP may result in administrator lockout.

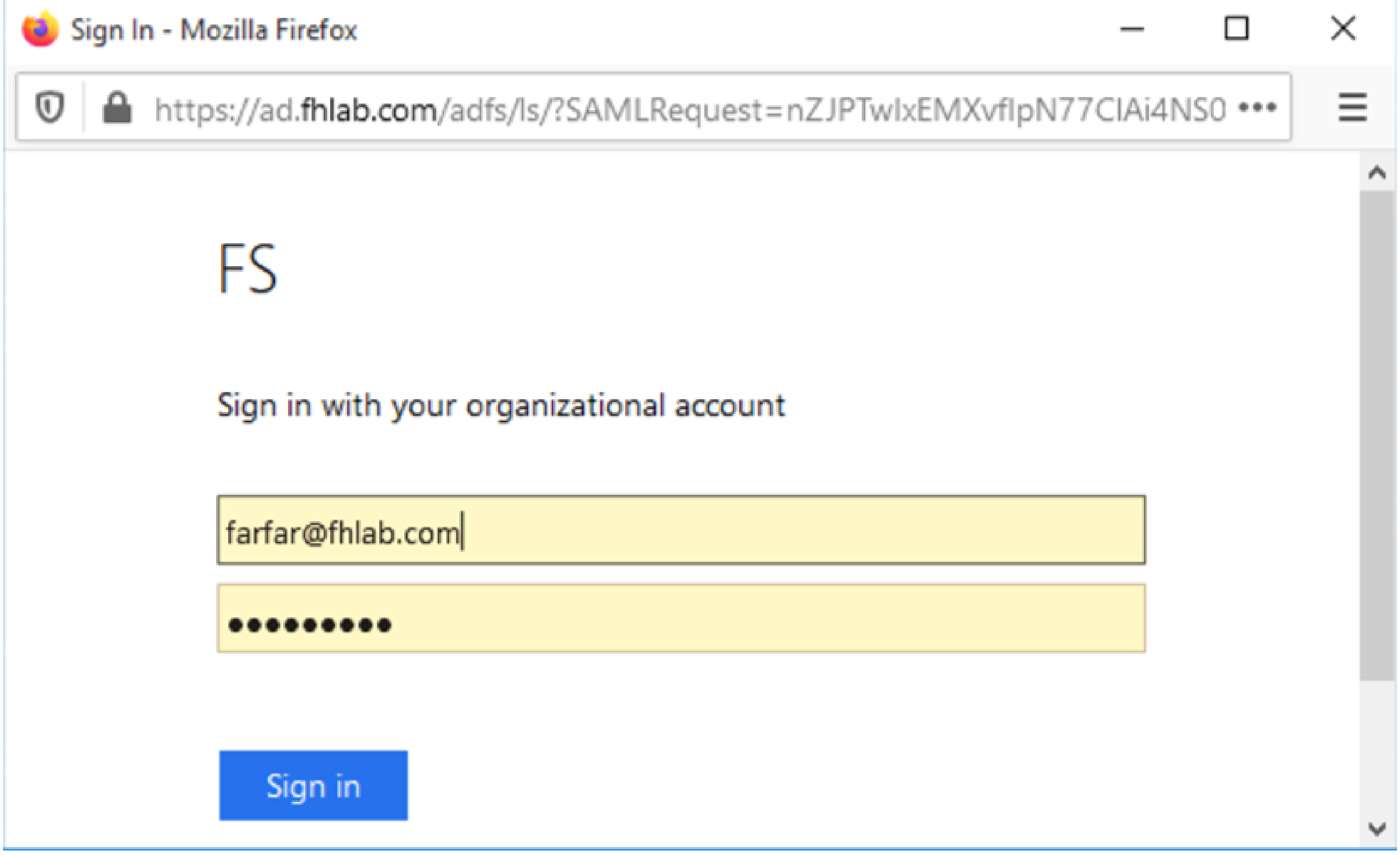
Valid administrator Usernames
farfar

2)Launch SSO test page

Run SSO Test...

Cancel

ユーザ認証ダイアログボックスが表示されたら、適切なユーザ名とパスワードでログインします。


Sign In - Mozilla Firefox
https://ad.fhlab.com/adfs/ls/?SAMLRequest=nZJPTwlxEMXvflpN77CIAi4NS0 •••
Sign in

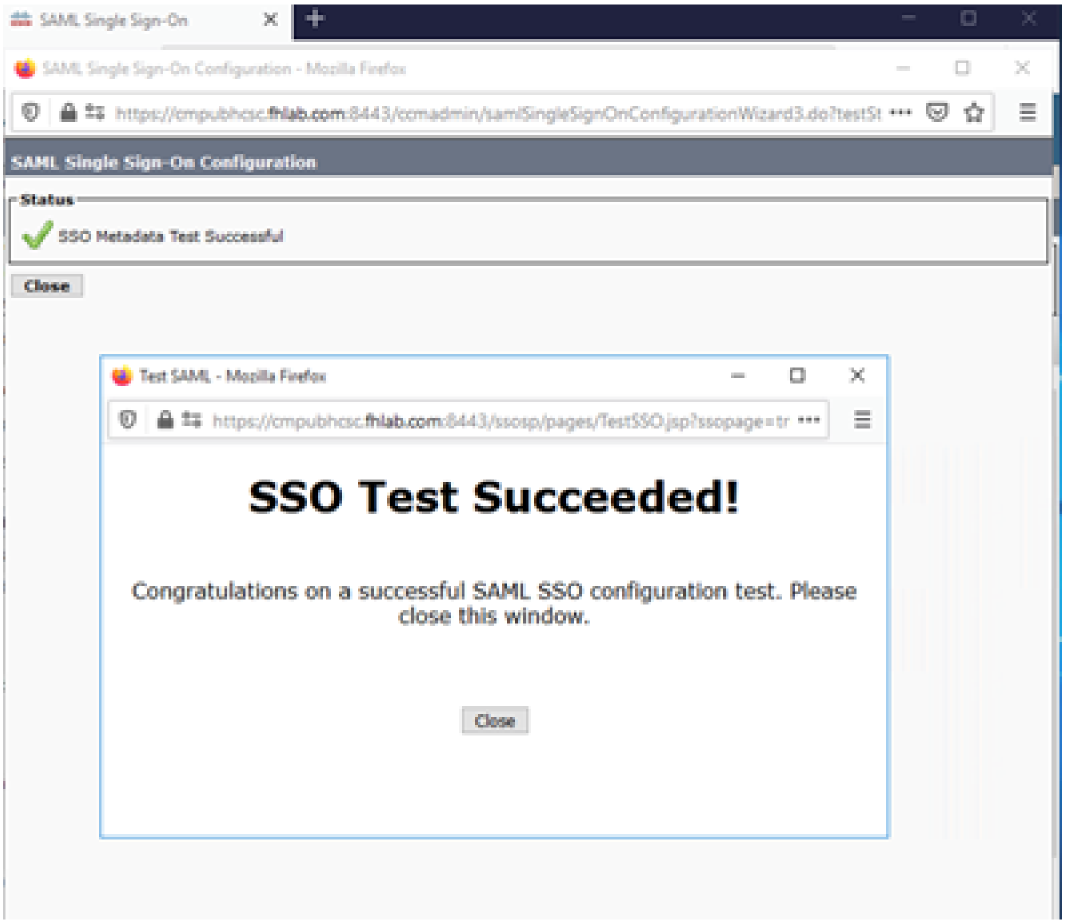
FS

Sign in with your organizational account

farfar@fhlab.com

●●●●●●●●●●

すべてが正しく設定されていれば、「SSO Test Succeeded!」というメッセージが表示されます。


SAML Single Sign-On
SAML Single Sign-On Configuration - Mozilla Firefox
https://cmpubhcsc.fhlab.com:8443/ccmadmin/samlSingleSignOnConfigurationWizard3.do?testSt •••
Close
Test SAML - Mozilla Firefox
https://cmpubhcsc.fhlab.com:8443/ssosp/pages/TestSSO.jsp?ssopage=tr •••
Close

SAML Single Sign-On Configuration

Status

✓ SSO Metadata Test Successful

SSO Test Succeeded!

Congratulations on a successful SAML SSO configuration test. Please close this window.

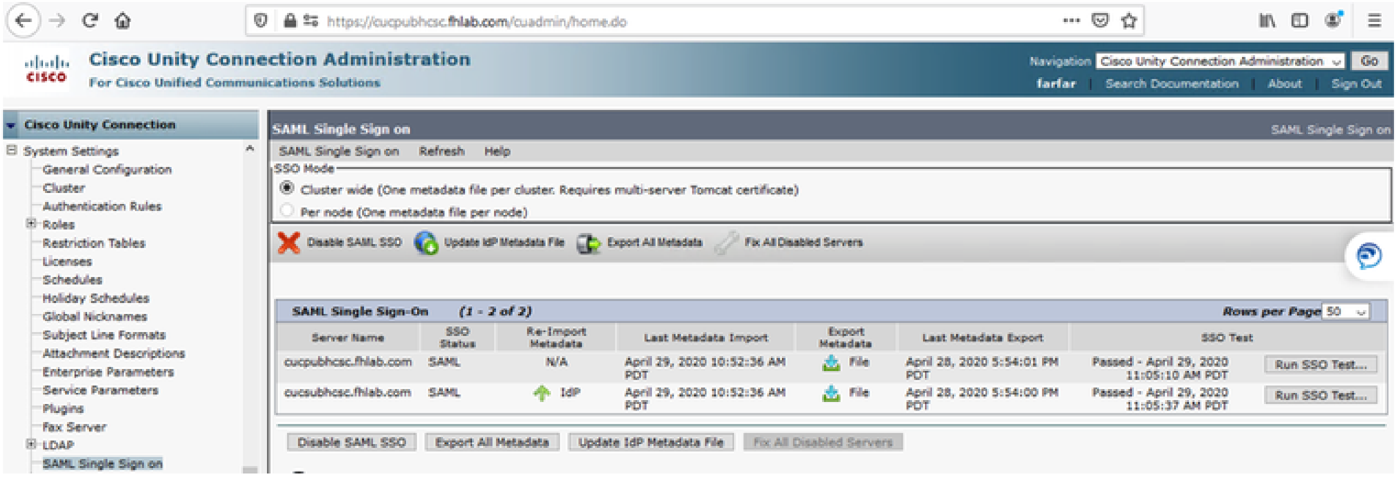
[Close] 、[Finish] の順にクリックして続行します。

これで、ADFSを使用してCUCMでSSOを有効にするための基本的な設定作業が完了しました。

CUCでのSSOの設定

Unity ConnectionでSSOを有効にするには、同じプロセスに従います。

CUCとのLDAP統合。



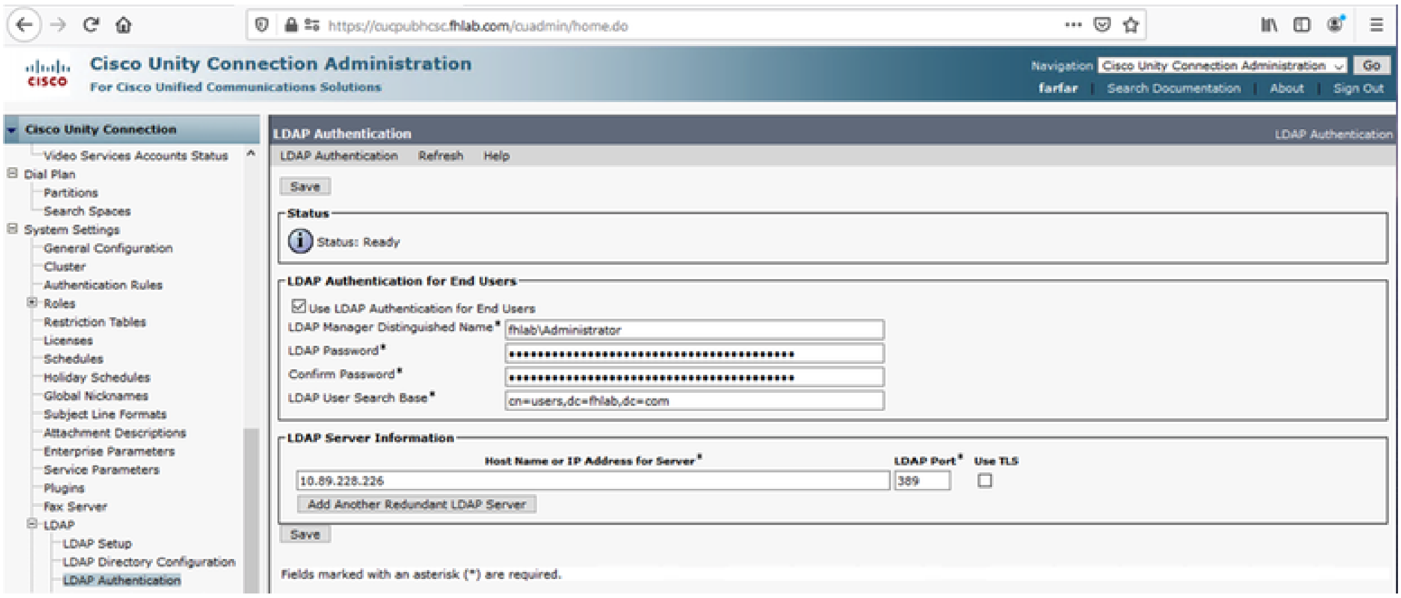
SAML Single Sign on

SSO Mode
- ● Cluster wide (One metadata file per cluster. Requires multi-server Tomcat certificate)
- ○ Per node (One metadata file per node)

SAML Single Sign-On (1 - 2 of 2) Rows per Page 50

Server Name	SSO Status	Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	SSO Test	
cucpubhcsc.fhlab.com	SAML	N/A	April 29, 2020 10:52:36 AM PDT	File	April 28, 2020 5:54:01 PM PDT	Passed - April 29, 2020 11:05:10 AM PDT	Run SSO Test...
cucsubhcsc.fhlab.com	SAML	IdP	April 29, 2020 10:52:36 AM PDT	File	April 28, 2020 5:54:00 PM PDT	Passed - April 29, 2020 11:05:37 AM PDT	Run SSO Test...

LDAP 認証の設定.



LDAP Authentication

Status
Status: Ready

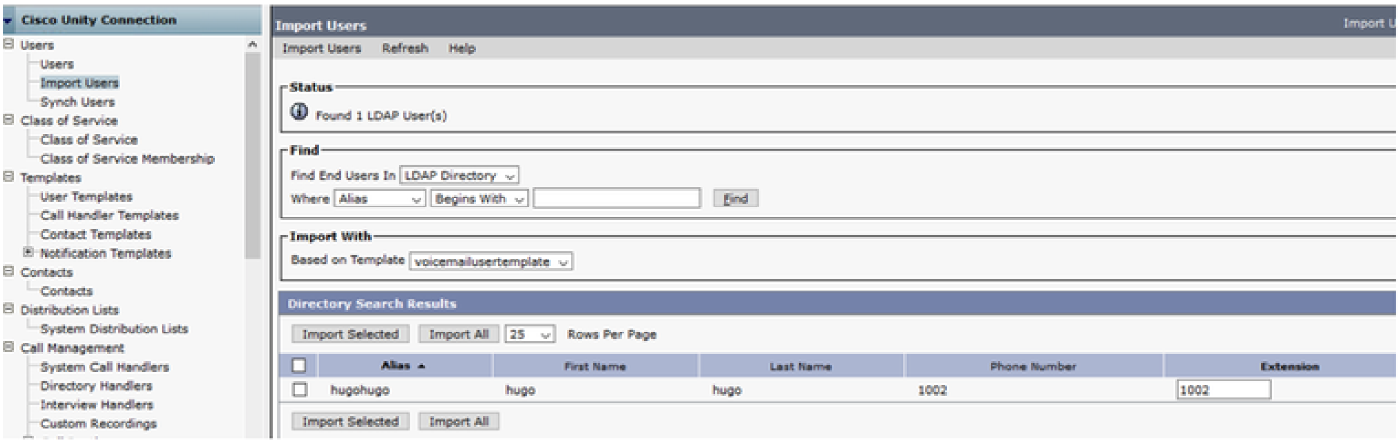
LDAP Authentication for End Users
☑ Use LDAP Authentication for End Users
LDAP Manager Distinguished Name* fhlab\Administrator
LDAP Password* ••
Confirm Password* ••
LDAP User Search Base* cn=users,dc=fhlab,dc=com

LDAP Server Information

Host Name or IP Address for Server*	LDAP Port*	Use TLS
10.89.228.226	389	□

Fields marked with an asterisk (*) are required.

ボイスメールが割り当てられるLDAPからのユーザと、SSOのテストに使用するユーザをインポートします。



Status
Found 1 LDAP User(s)

Find End Users In: LDAP Directory
Where: Alias, Begins With

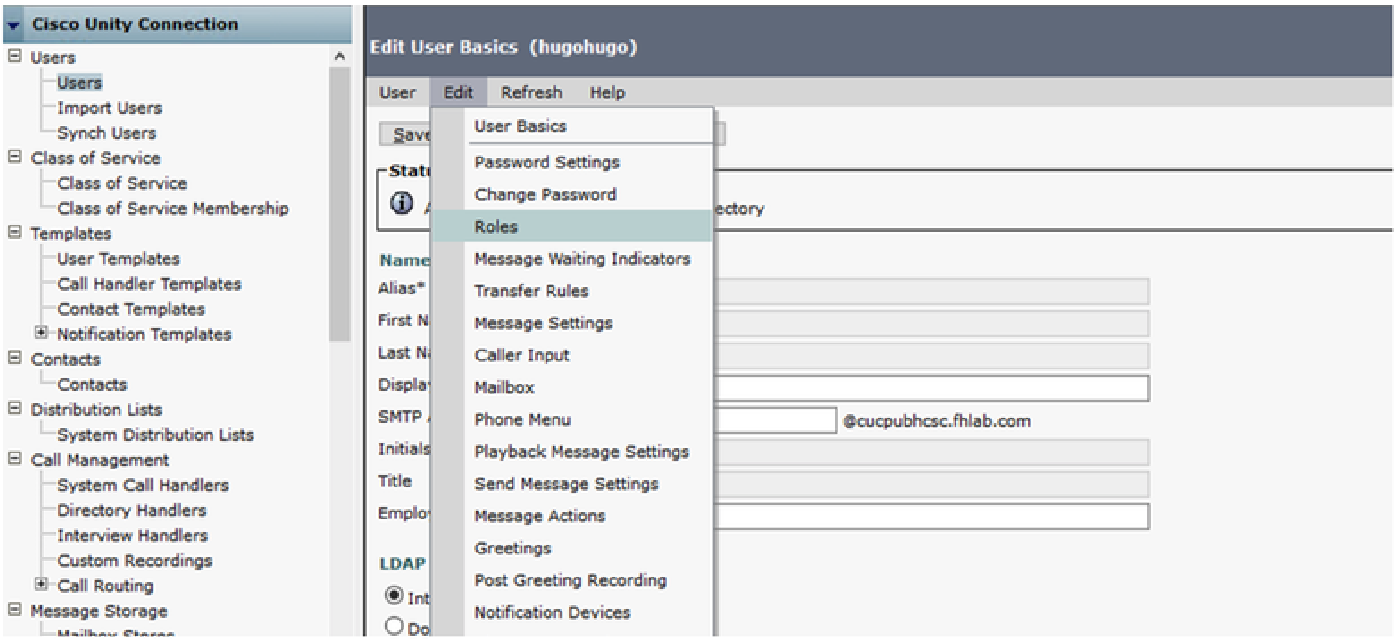
Import With
Based on Template: voicemailusertemplate

Directory Search Results

Rows Per Page: 25

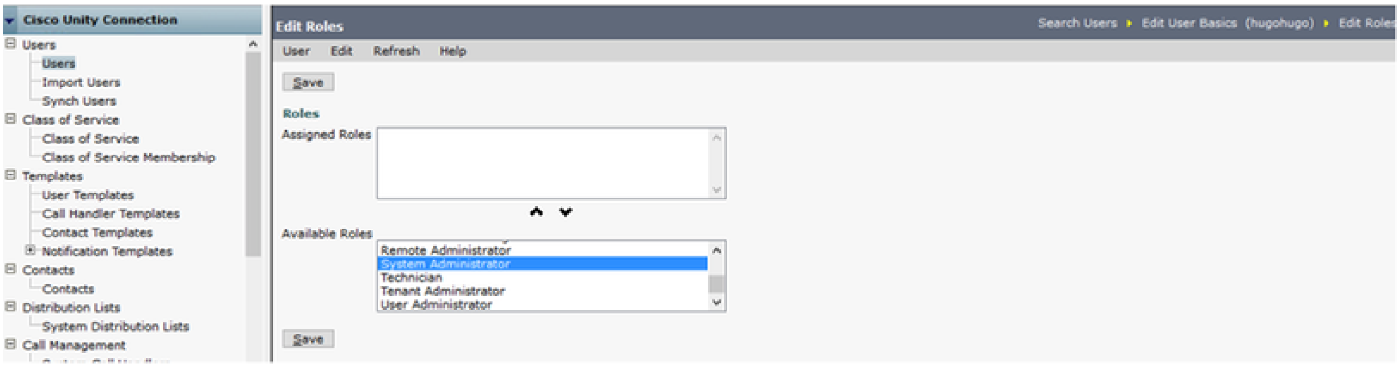
□	Alias ▲	First Name	Last Name	Phone Number	Extension
□	hugohugo	hugo	hugo	1002	1002

図に示すように、[Users] > [Edit] > [Roles]に移動します。



SMTP: @cucpubhcsc.fhlab.com

テストユーザにシステム管理者の役割を割り当てます。



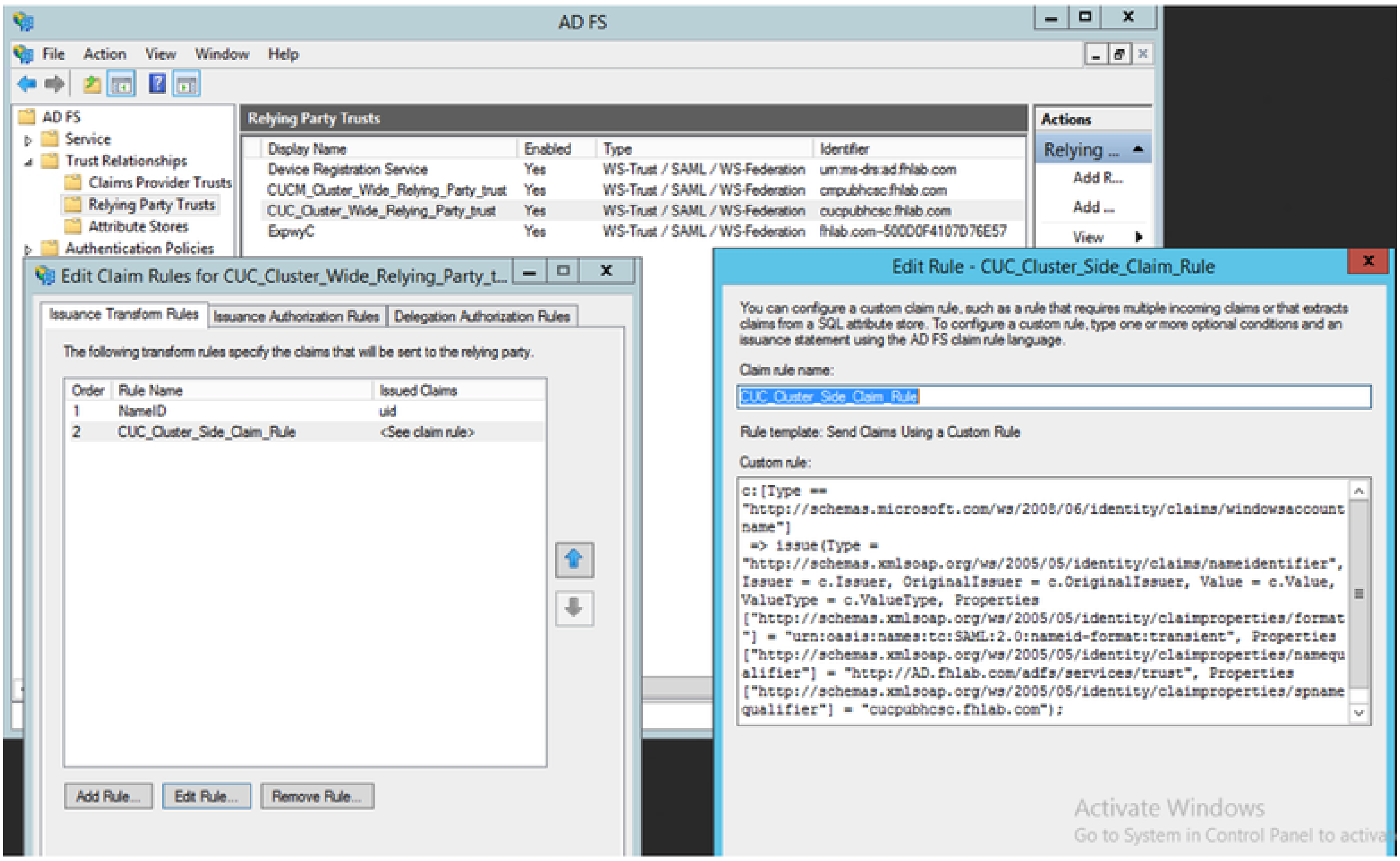
Roles

Assigned Roles:

Available Roles:
Remote Administrator
System Administrator
Technician
Tenant Administrator
User Administrator

CUCメタデータ

これでCUCメタデータがダウンロードされ、CUC用RelyingPartyTrustが作成され、CUCメタデータがアップロードされ、ADFS 3.0でI AD FSルールが作成されました



Display Name	Enabled	Type	Identifier
Device Registration Service	Yes	WS-Trust / SAML / WS-Federation	urn:ms-drs:ad.fhlab.com
CUCM_Cluster_Wide_Relying_Party_trust	Yes	WS-Trust / SAML / WS-Federation	cmpubhcsc.fhlab.com
CUC_Cluster_Wide_Relying_Party_trust	Yes	WS-Trust / SAML / WS-Federation	cucpubhcsc.fhlab.com
ExpwyC	Yes	WS-Trust / SAML / WS-Federation	fhlab.com-500D0F4107D76E57

Edit Claim Rules for CUC_Cluster_Wide_Relying_Party_t...

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims
1	NameID	uid
2	CUC_Cluster_Side_Claim_Rule	<See claim rule>

Edit Rule - CUC_Cluster_Side_Claim_Rule

You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS claim rule language.

Claim rule name:
CUC_Cluster_Side_Claim_Rule

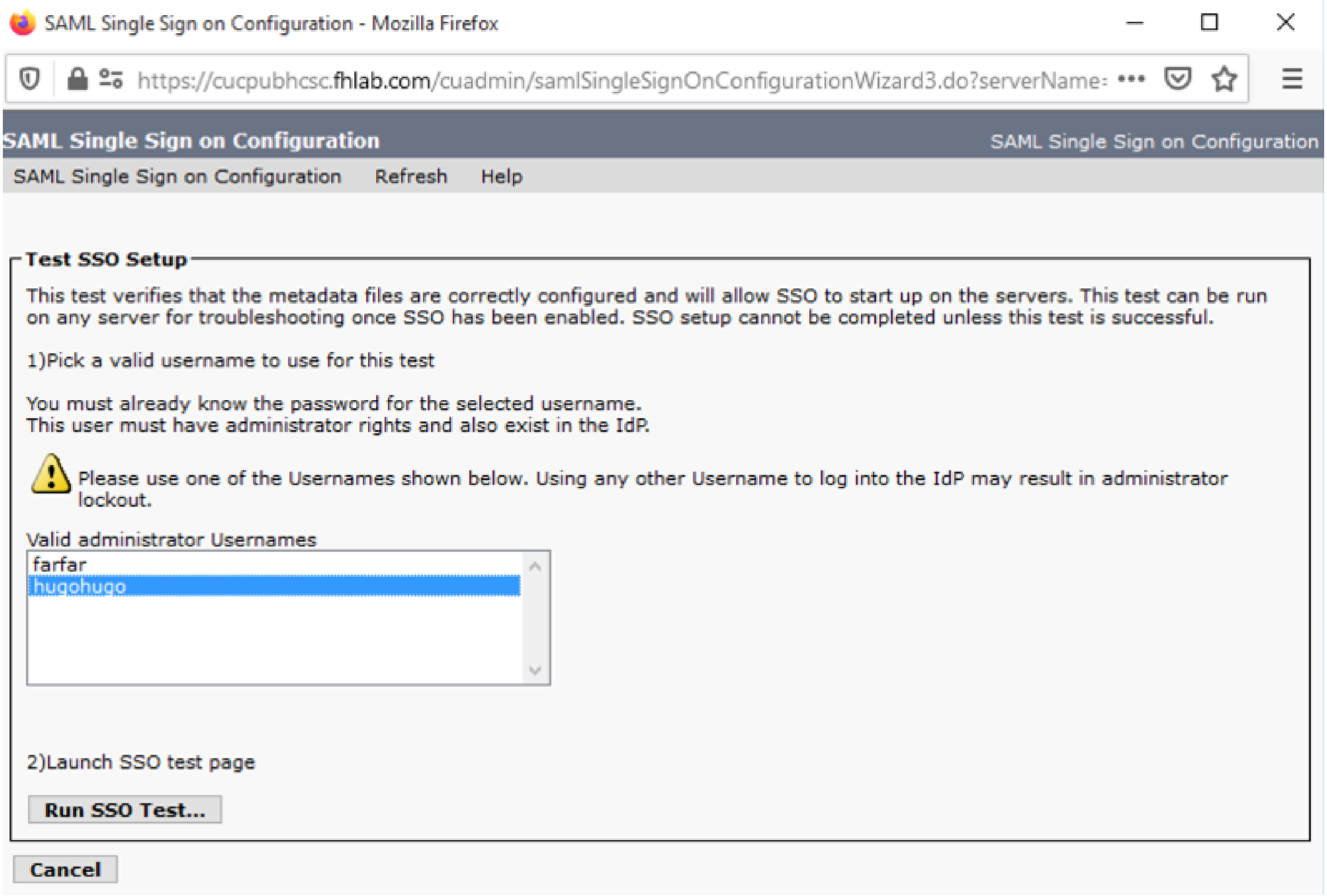
Rule template: Send Claims Using a Custom Rule

Custom rule:

```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccount
name"]
 => issue(Type =
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value,
ValueType = c.ValueType, Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format
"] = "urn:oasis:names:tc:SAML:2.0:nameid-format:transient", Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequ
alifier"] = "http://AD.fhlab.com/adfs/services/trust", Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spname
qualifier"] = "cucpubhcsc.fhlab.com");
```

Activate Windows
Go to System in Control Panel to activa

[SAML Single Sign-On]に移動し、[Enable SAML SSO]を有効にします。


SAML Single Sign on Configuration - Mozilla Firefox
https://cucpubhcsc.fhlab.com/cuadmin/samlSingleSignOnConfigurationWizard3.do?serverName:
SAML Single Sign on Configuration
SAML Single Sign on Configuration
SAML Single Sign on Configuration
Refresh
Help

Test SSO Setup

This test verifies that the metadata files are correctly configured and will allow SSO to start up on the servers. This test can be run on any server for troubleshooting once SSO has been enabled. SSO setup cannot be completed unless this test is successful.

1)Pick a valid username to use for this test

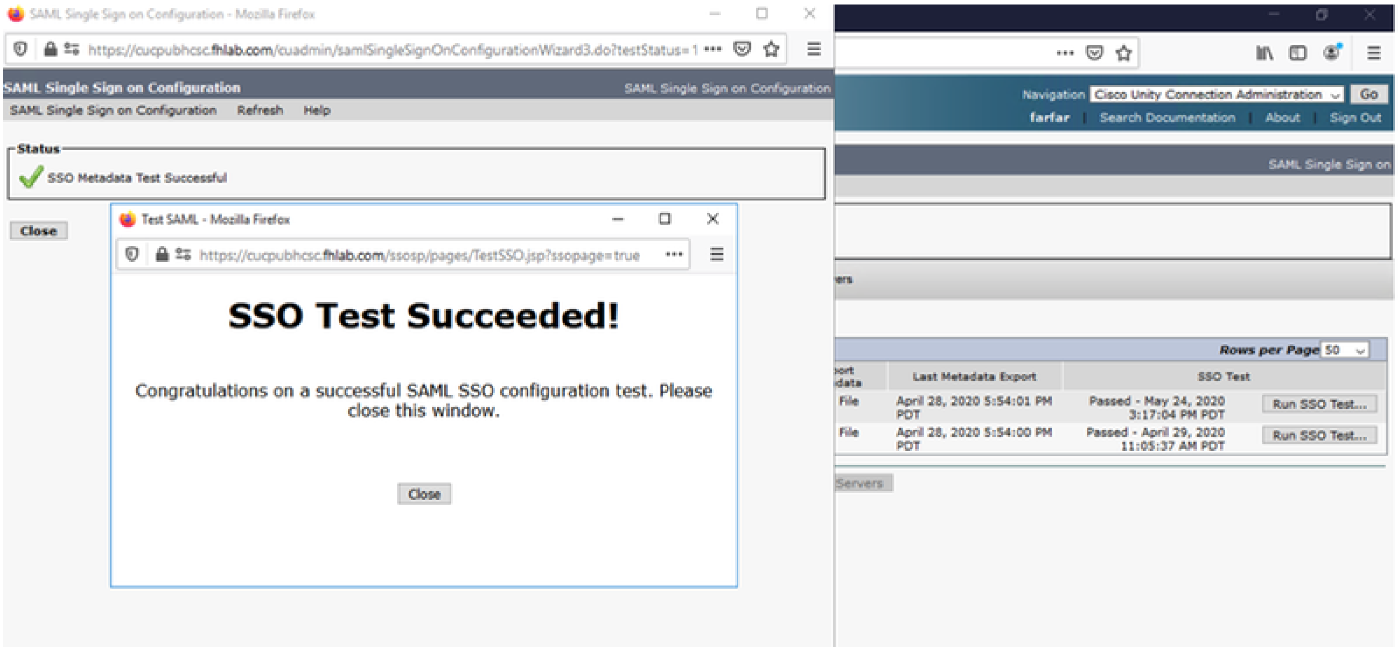
You must already know the password for the selected username.
This user must have administrator rights and also exist in the IdP.

⚠ Please use one of the Usernames shown below. Using any other Username to log into the IdP may result in administrator lockout.

Valid administrator Usernames

farfar
hugohugo

2)Launch SSO test page



SAML Single Sign on Configuration - Mozilla Firefox
https://cucpubhcsc.fhlab.com/cuadmin/samlSingleSignOnConfigurationWizard3.do?testStatus=1
SAML Single Sign on Configuration
SAML Single Sign on Configuration
SAML Single Sign on Configuration
Refresh
Help
Status
Close
Test SAML - Mozilla Firefox
https://cucpubhcsc.fhlab.com/ssosp/pages/TestSSO.jsp?ssopage=true
Close
Navigation
Cisco Unity Connection Administration
Go
farfar
Search Documentation
About
Sign Out
SAML Single Sign on
Rows per Page
50
Servers

SSO Metadata Test Successful

SSO Test Succeeded!

Congratulations on a successful SAML SSO configuration test. Please close this window.

ort data	Last Metadata Export	SSO Test	
File	April 28, 2020 5:54:01 PM PDT	Passed - May 24, 2020 3:17:04 PM PDT	Run SSO Test...
File	April 28, 2020 5:54:00 PM PDT	Passed - April 29, 2020 11:05:37 AM PDT	Run SSO Test...

ExpresswayでのSSOの設定

Expressway Cへのメタデータのインポート

ブラウザでhttps://<ADFS FQDN>/FederationMetadata/2007-06/FederationMetadata.xmlを開き、メタデータをローカルフォルダに保存します

[Configuration] > [**Unified Communications] > [IDP]にアップロードします。**

Expressway Cからメタデータをエクスポート

[configuration] -> [Unified Communications] -> [IDP] -> [Export SAML Data]に移動します。

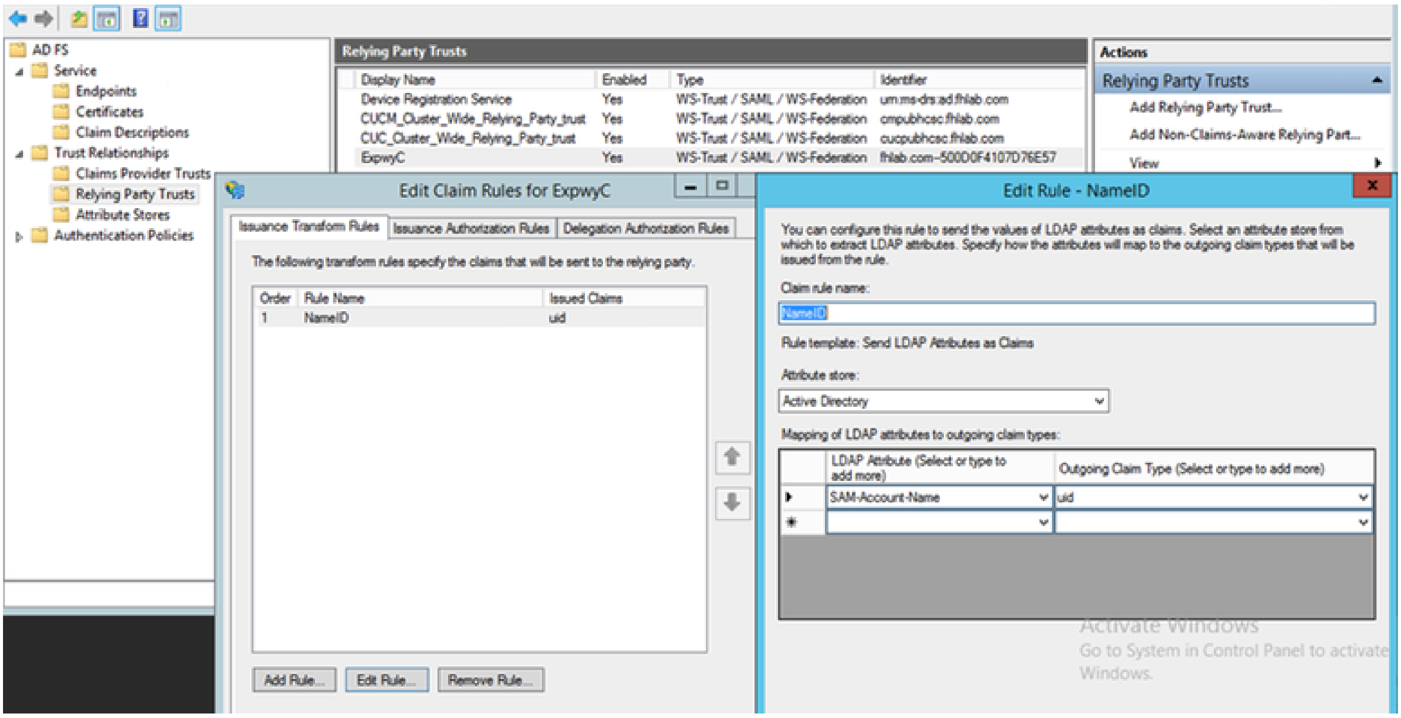
クラスタモードでは、SAMLに含まれる自己署名証明書（長いライフタイムを含む）が使用されます

SAML要求の署名に使用されるメタデータ

- クラスタ全体のモードで、単一のクラスタ全体のメタデータ· ファイルをダウンロードするには、「ダウンロード」をクリックします
- ピア単位モードで、個々のピアのメタデータファイルをダウンロードするには、ピアの横にある[Download]をクリックします。すべて.zipファイルにエクスポートするには、[すべてダウンロード(Download All)]をクリックします。

Cisco Expressway-Eの証明書利用者信頼の追加

まず、Expressway-Eの証明書利用者信頼を作成し、次にIDをUID属性として送信する要求ルールを追加します。



Relying Party Trusts

Display Name	Enabled	Type	Identifier
Device Registration Service	Yes	WS-Trust / SAML / WS-Federation	urn:ms-drs:ad.fhlab.com
CUCM_Cluster_Wide_Relying_Party_trust	Yes	WS-Trust / SAML / WS-Federation	cmpubhcsc.fhlab.com
CUC_Cluster_Wide_Relying_Party_trust	Yes	WS-Trust / SAML / WS-Federation	cucpubhcsc.fhlab.com
ExpwyC	Yes	WS-Trust / SAML / WS-Federation	fhlab.com-500D0F4107D76E57

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims
1	NameID	uid

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name: NameID

Rule template: Send LDAP Attributes as Claims

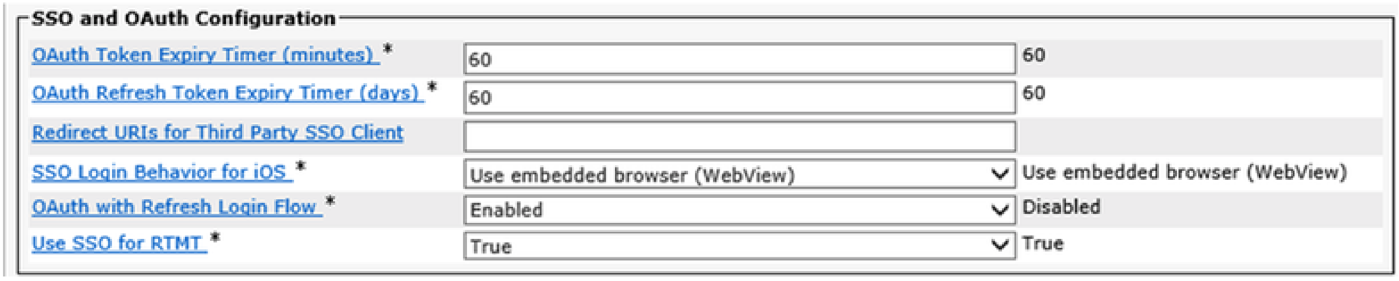
Attribute store: Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▸	SAM-Account-Name	uid
*		

ログインの更新によるOAuth

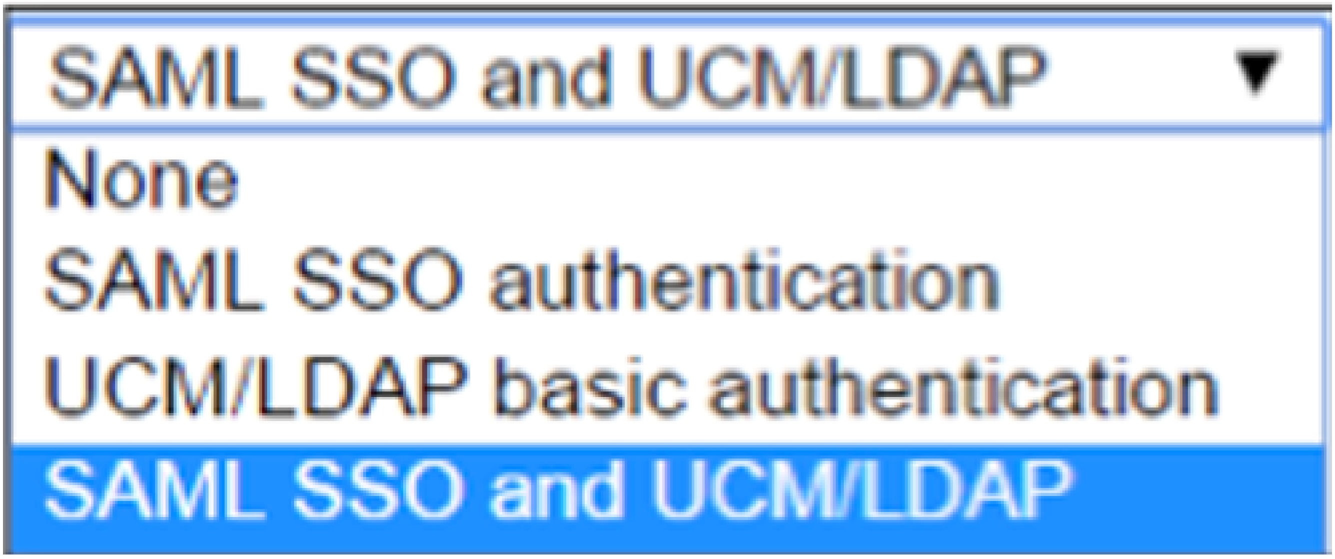
Cisco CUCMエンタープライズパラメータで、[Refresh login flow parameter]が有効になっていることを確認します。[**Cisco Unified CM Administration**] > [**Enterprise Parameters**] > [**SSO and OAuth Configuration**]**に移動します。**



SSO and OAuth Configuration

OAuth Token Expiry Timer (minutes) *	60	60
OAuth Refresh Token Expiry Timer (days) *	60	60
Redirect URIs for Third Party SSO Client		
SSO Login Behavior for iOS *	Use embedded browser (WebView)	Use embedded browser (WebView)
OAuth with Refresh Login Flow *	Enabled	Disabled
Use SSO for RTMT *	True	True

認証パス



- 認証パスが「SAML SSO認証」に設定されている場合、SSO対応のUnified CMクラスタを使

用するJabberクライアントだけが、このExpresswayでMRAを使用できます。これはSSOのみの設定です。
- すべてのIP電話、すべてのTelePresenceエンドポイント、およびSSOが設定されていないUnified CMクラスタにホーム接続されているJabberクライアントに対するExpressway MRAのサポートには、UCM/LDAP認証を含める認証パスが必要があります。
- 1つ以上のUnified CMクラスタがJabber SSOをサポートしている場合は、[SAML SSOおよびUCM/LDAP]を選択して、SSOと基本認証の両方を許可します。

SSOアーキテクチャ

SAMLは、XMLベースのオープンスタンダードなデータ形式で、管理者がいずれかのアプリケーションにサインインした後、定義済みのシスココラボレーションアプリケーションにシームレスにアクセスできるようにします。SAML SSOは、SAML 2.0プロトコルを使用して、シスココラボレーションソリューションのクロスドメインおよびクロスプロダクトシングルサインオンを提供します。

オンプレミスのログインフロー

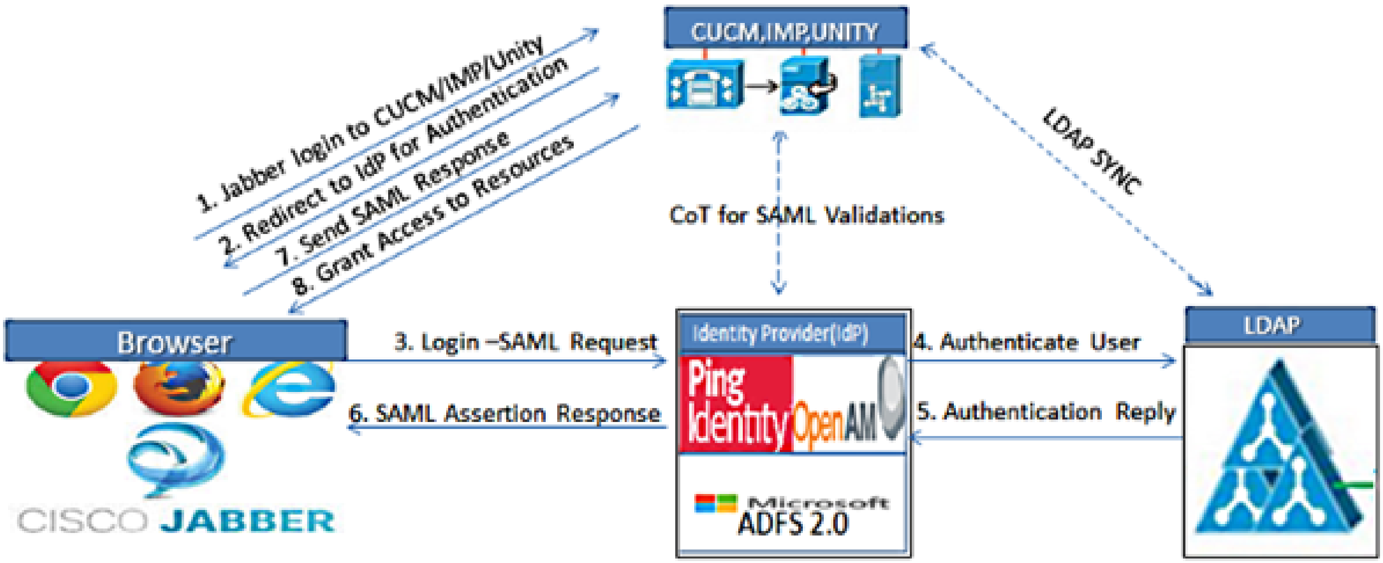
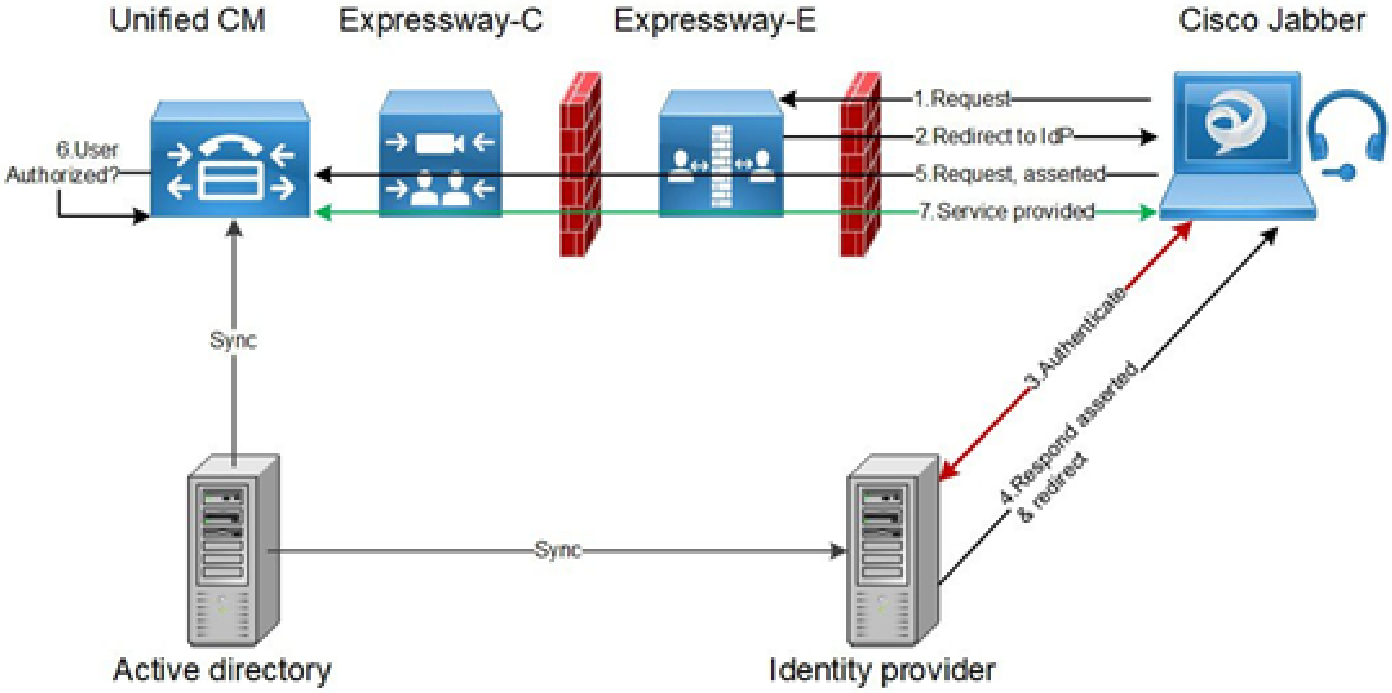


Figure :SAML Single sign SSO Call Flow for Collaboration Servers

MRAログインフロー



OAuth

OAuthは認可をサポートする標準です。ユーザを認証する前に、ユーザを認証する必要があります。認証コード許可フローは、クライアントがリソース（Unified CM、IM&P、Unity、およびExpresswayサービス）にアクセスするためのアクセストークンを取得し、更新する方法を提供します。 このフローはリダイレクションにも基づいているため、クライアントがユーザによって制御されるHTTPユーザエージェント（Webブラウザ）と対話できる必要があります。クライアントは、HTTPSを使用して認証サーバに対して最初の要求を行います。OAuthサーバは、ユーザを認証サービスにリダイレクトします。SAML SSOが有効になっている場合は、Unified CMまたは外部IdPで実行されている可能性があります。使用されている認証方法によっては、エンドユーザにWebページビューが表示され、自身を認証できます。（Kerberos認証は、Webページを表示しない例です）。 暗黙の許可フローとは異なり、認証コードの許可フローが成功すると、OAuthサーバはWebブラウザに「許可コード」を発行します。これは、Webブラウザからクライアントに返される、一時的な一意のコードです。クライアントは、この「認証コード」を事前共有秘密とともに認証サーバに提供し、「アクセストークン」と「リフレッシュトークン」を交換して受信します。この手順で使用するクライアントシークレットにより、認証サービスは、登録および認証されたクライアントのみに使用を制限できます。トークンは次の目的で使用されます。

アクセス/更新トークン

アクセストークン：このトークンは、認証サーバによって発行されます。クライアントは、そのサーバ上の保護されたリソースにアクセスする必要がある場合、そのサーバにトークンを提示します。リソースサーバは、トークンを使用してトークンを検証し、接続を信頼できます。（Ciscoアクセストークンのデフォルトは60分です）

トークンの更新：このトークンは、認証サーバによって再度発行されます。クライアントは、アクセストークンの有効期限が切れたか、期限が切れたときに、クライアントシークレットとともに、このトークンを認証サーバに提示します。更新トークンがまだ有効な場合、認証サーバは別の認証を必要とせずに新しいアクセストークンを発行します。（シスコの更新トークンは、デフォルトで60日間のライフタイムに設定されています）。 更新トークンの有効期限が切れた場合は、新しいトークンを取得するために、新しい完全なOAuth承認コード許可フローを開始する必要があります。

OAuth承認コード認可フローが改善されました

暗黙の許可フローでは、アクセストークンはHTTPユーザエージェント（ブラウザ）を介してJabberクライアントに渡されます。 認証コード許可フローでは、認証サーバとJabberクライアントの間でアクセストークンが直接交換されます。トークンは、時間制限された一意の認証コードを使用して認証サーバから要求されます。このアクセストークンの直接交換は、より安全で、リスクの発生を軽減します。

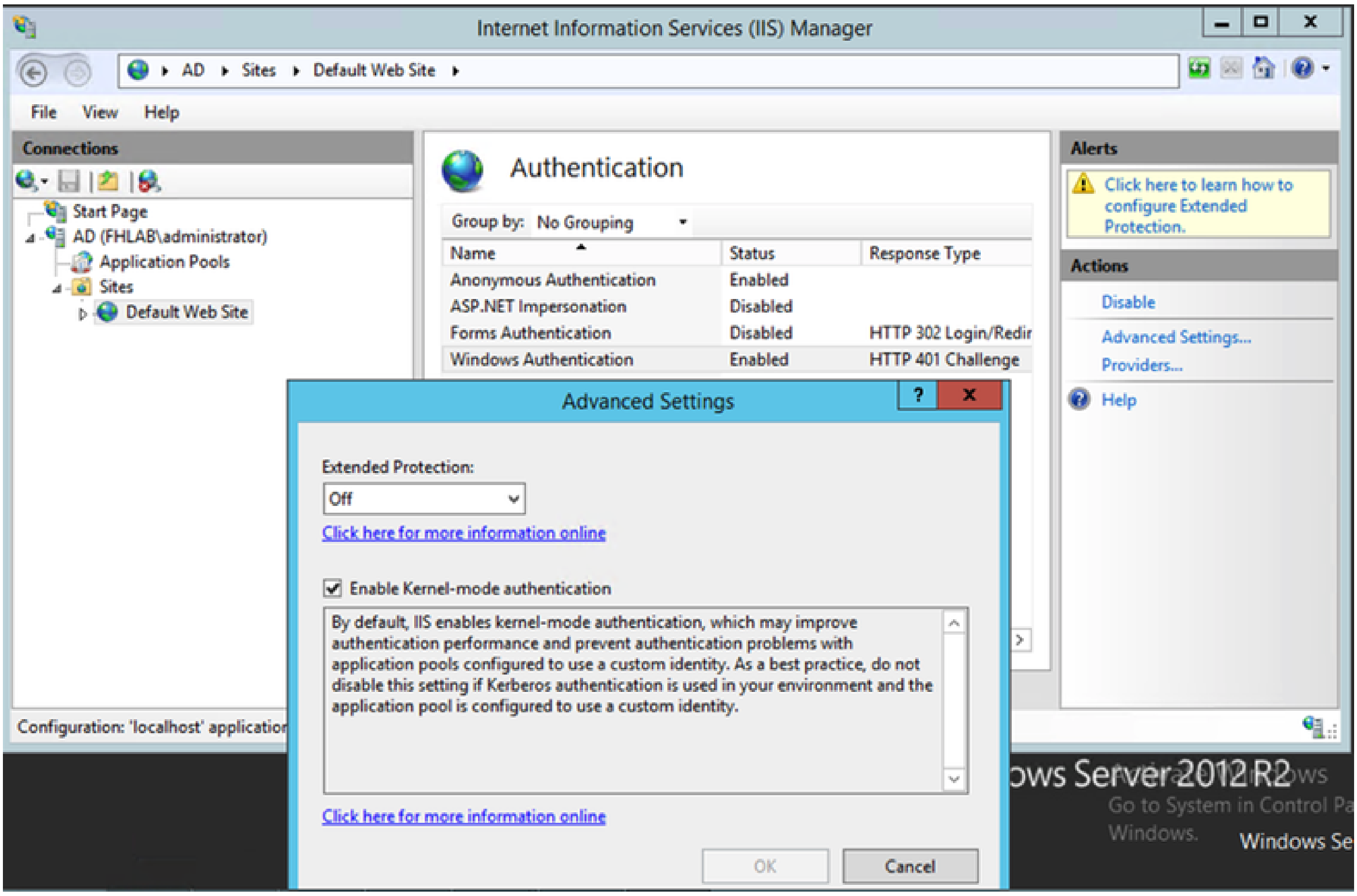
OAuth承認コード許可フローは、更新トークンの使用をサポートします。これにより、エンドユーザは頻繁に再認証する必要がないため（デフォルトでは60日）、エンドユーザのエクスペリエンスが向上します

Kerberosの設定

[Windows Authentication]を選択します

インターネットインフォメーションサービス(IIS)マネージャ>サイト>デフォルトのWebサイト>認証> Windows認証>詳細設定。

1. [Enable Kernel-mode authentication]をオフにします。
2. [Extended Protection]が[Off]になっていることを確認します。



Authentication

Group by: No Grouping

Name	Status	Response Type
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Disabled	
Forms Authentication	Disabled	HTTP 302 Login/Redir
Windows Authentication	Enabled	HTTP 401 Challenge

Click here to learn how to configure Extended Protection.

Advanced Settings

Extended Protection: Off

Click here for more information online

☑ Enable Kernel-mode authentication

By default, IIS enables kernel-mode authentication, which may improve authentication performance and prevent authentication problems with application pools configured to use a custom identity. As a best practice, do not disable this setting if Kerberos authentication is used in your environment and the application pool is configured to use a custom identity.

Click here for more information online

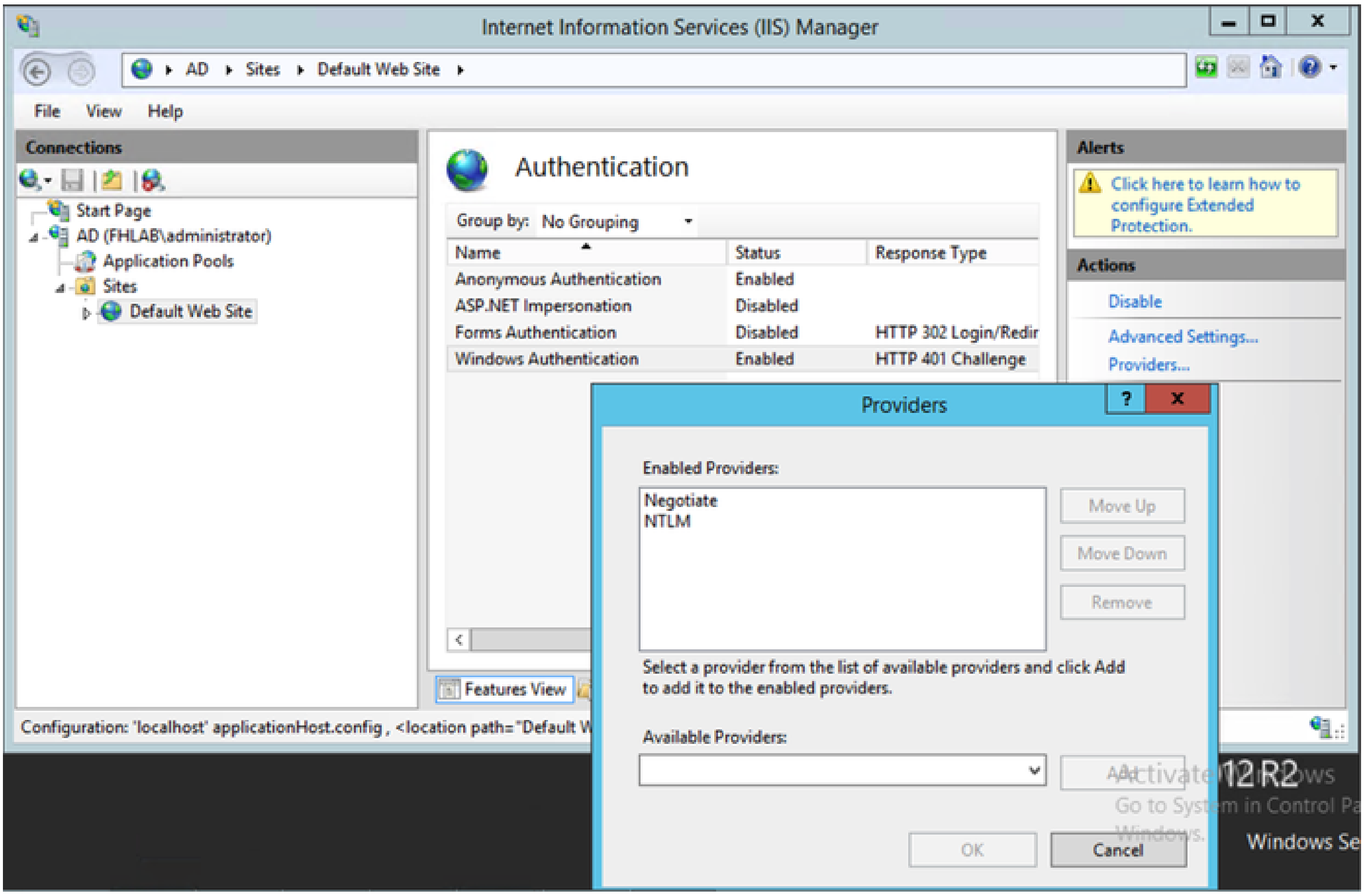
OK Cancel

ADFSは両方のKerberos NTLMをサポート

Windows 以外のすべてのクライアントは、Kerberos を使用できず、NTLM に依存するため、AD FS バージョン 3.0 が Kerberos プロトコルと NT LAN Manager （NTLM）プロトコルの両方をサ

ポートすることを確認します。

右側のペインで[Providers]を選択し、[Enabled Providers]に[Negotiate]と[NTLM]が表示されていることを確認します。



Internet Information Services (IIS) Manager

AD ▸ Sites ▸ Default Web Site ▸

Authentication

Group by: No Grouping

Name	Status	Response Type
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Disabled	
Forms Authentication	Disabled	HTTP 302 Login/Redir
Windows Authentication	Enabled	HTTP 401 Challenge

Click here to learn how to configure Extended Protection.

Providers

Enabled Providers:

Negotiate
NTLM

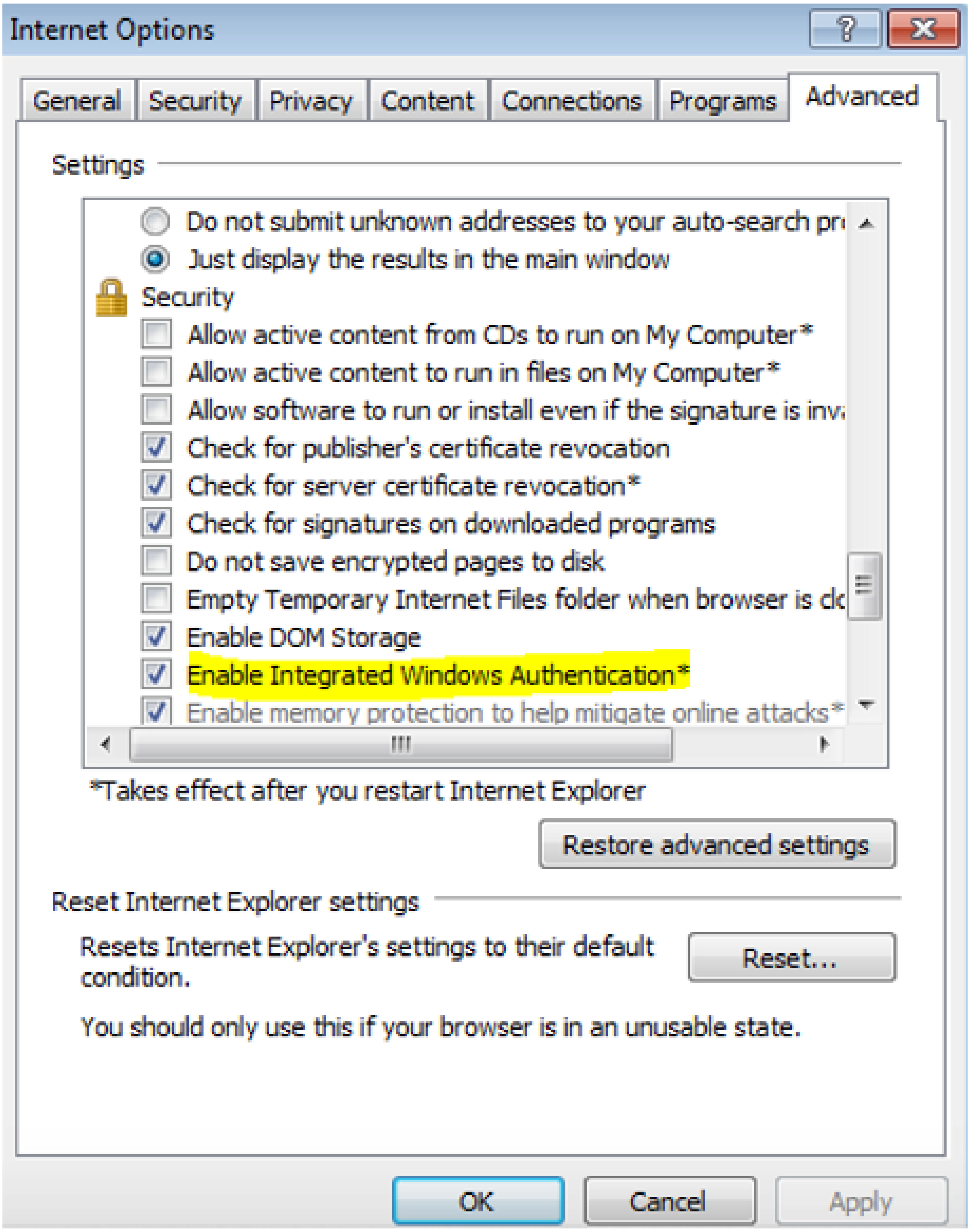
Select a provider from the list of available providers and click Add to add it to the enabled providers.

Available Providers:

Configuration: 'localhost' applicationHost.config , <location path="Default W

Microsoft Internet Explorerの設定

[Internet Explorer] > [Advanced] > [Enable Integrated Windows Authentication] がオンになっていることを確認します。



Settings

○ Do not submit unknown addresses to your auto-search pr

● Just display the results in the main window

Security

□ Allow active content from CDs to run on My Computer*

□ Allow active content to run in files on My Computer*

□ Allow software to run or install even if the signature is inv

☑ Check for publisher's certificate revocation

☑ Check for server certificate revocation*

☑ Check for signatures on downloaded programs

□ Do not save encrypted pages to disk

□ Empty Temporary Internet Files folder when browser is clo

☑ Enable DOM Storage

☑ Enable Integrated Windows Authentication*

☑ Enable memory protection to help mitigate online attacks*

*Takes effect after you restart Internet Explorer

Reset Internet Explorer settings

Resets Internet Explorer's settings to their default condition.

You should only use this if your browser is in an unusable state.

[Security] > [Intranet zones] > [Sites]でADFS URLを追加します